

CYBER SECURITY: RECOVERY AND RECONSTITUTION OF CRITICAL NETWORKS

HEARING

BEFORE THE

FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, AND INTERNATIONAL
SECURITY SUBCOMMITTEE

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 28, 2006

Available via <http://www.access.gpo.gov/congress/senate>

Printed for the use of the Committee on Homeland Security
and Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

29-759 PDF

WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

| | |
|---------------------------------|----------------------------------|
| TED STEVENS, Alaska | JOSEPH I. LIEBERMAN, Connecticut |
| GEORGE V. VOINOVICH, Ohio | CARL LEVIN, Michigan |
| NORM COLEMAN, Minnesota | DANIEL K. AKAKA, Hawaii |
| TOM COBURN, Oklahoma | THOMAS R. CARPER, Delaware |
| LINCOLN D. CHAFEE, Rhode Island | MARK DAYTON, Minnesota |
| ROBERT F. BENNETT, Utah | FRANK LAUTENBERG, New Jersey |
| PETE V. DOMENICI, New Mexico | MARK PRYOR, Arkansas |
| JOHN W. WARNER, Virginia | |

MICHAEL D. BOPP, *Staff Director and Chief Counsel*

MICHAEL L. ALEXANDER, *Minority Staff Director*

TRINA DRIESSNACK TYRER, *Chief Clerk*

FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, AND
INTERNATIONAL SECURITY SUBCOMMITTEE

TOM COBURN, Oklahoma, *Chairman*

| | |
|---------------------------------|------------------------------|
| TED STEVENS, Alaska | THOMAS CARPER, Delaware |
| GEORGE V. VOINOVICH, Ohio | CARL LEVIN, Michigan |
| LINCOLN D. CHAFEE, Rhode Island | DANIEL K. AKAKA, Hawaii |
| ROBERT F. BENNETT, Utah | MARK DAYTON, Minnesota |
| PETE V. DOMENICI, New Mexico | FRANK LAUTENBERG, New Jersey |
| JOHN W. WARNER, Virginia | MARK PRYOR, Arkansas |

KATY FRENCH, *Staff Director*

SHEILA MURPHY, *Minority Staff Director*

JOHN KILVINGTON, *Minority Deputy Staff Director*

LIZ SCRANTON, *Chief Clerk*

CONTENTS

| | |
|----------------------|------|
| Opening statements: | Page |
| Senator Coburn | 1 |

WITNESSES

FRIDAY, JULY 28, 2006

| | |
|-----------------------------------------------------------------------------------------------------------------------------------|----|
| George Foresman, Under Secretary for Preparedness, U.S. Department of Homeland Security | 5 |
| Richard C. Schaeffer, Jr., Director of Information Assurance, National Security Agency | 7 |
| Karen Evans, Administrator for Electronic Government and Information Technology, Office of Management and Budget | 9 |
| Keith Rhodes, Chief Technologist and Director, Center for Technology and Engineering, U.S. Government Accountability Office | 10 |
| Thomas E. Noonan, President and Chief Executive Officer, Internet Security Systems | 20 |
| Roberta A. Bienfait, Senior Vice President, Global Network Operations, AT&T | 22 |
| Michael A. Aisenberg, Director of Government Relations, VeriSign, Inc., and Vice Chair, IT Sector Coordinating Council | 24 |
| Karl Brondell, State Farm Insurance Companies, on behalf of the Business Roundtable | 26 |

ALPHABETICAL LIST OF WITNESSES

| | |
|---------------------------------------------|-----|
| Aisenberg, Michael A.: | |
| Testimony | 24 |
| Prepared statement | 161 |
| Bienfait, Roberta A.: | |
| Testimony | 22 |
| Prepared statement | 139 |
| Brondell, Karl: | |
| Testimony | 26 |
| Prepared statement | 167 |
| Evans, Karen: | |
| Testimony | 9 |
| Prepared statement with an attachment | 53 |
| Foresman, George: | |
| Testimony | 5 |
| Prepared statement | 33 |
| Noonan, Thomas E.: | |
| Testimony | 20 |
| Prepared statement | 132 |
| Rhodes, Keith: | |
| Testimony | 10 |
| Prepared statement | 111 |
| Schaeffer, Richard C., Jr.: | |
| Testimony | 7 |
| Prepared statement | 50 |

APPENDIX

| | |
|---------------------------------------------------------------------------------------------------------------------|-----|
| Hon. Thomas Jarrett, Secretary and CIO, Delaware Department of Technology and Information, prepared statement | 174 |
|---------------------------------------------------------------------------------------------------------------------|-----|

IV

| | Page |
|----------------------------------------------|------|
| Questions and responses for the Record from: | |
| Mr. Foresman | 181 |
| Mr. Schaeffer | 197 |
| Mr. Evans | 200 |
| Mr. Rhodes | 209 |
| Mr. Bienfait | 213 |
| Mr. Aisenberg | 223 |
| Mr. Brondell | 226 |

CYBER SECURITY: RECOVERY AND RECONSTITUTION OF CRITICAL NETWORKS

FRIDAY, JULY 28, 2006

U.S. SENATE,
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT
INFORMATION, AND INTERNATIONAL SECURITY,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:35 a.m., in room 342, Dirksen Senate Office Building, Hon. Tom Coburn, Chairman of the Subcommittee, presiding.

Present: Senator Coburn.

OPENING STATEMENT OF CHAIRMAN COBURN

Chairman COBURN. The Subcommittee on Federal Financial Management, Government Information, and International Security will come to order.

Today's hearing is titled "Cyber Security: Recovery and Reconstitution of Critical Networks." This is the second hearing in a series we will be conducting on cyber security. It is actually the third. We have had a high-level secured briefing and hearing on this, as well. On July 19, 2005, this Subcommittee held a hearing on the importance of cyber security to our Nation's critical infrastructures. The hearing highlighted the importance of forging a public-private, and I will emphasize private, partnership to protect critical infrastructure and focused on challenges facing the Department of Homeland Security (DHS) in facilitating and leveraging such partnerships.

Things that we have learned through the September 11 terrorist attacks and the response to Hurricane Katrina further emphasize these challenges. Today, despite spending millions of dollars over the past year, DHS continues to struggle with how to effectively form and maintain effective public-private partnerships in support of cyber security, including how to protect Internet infrastructure and how to recover it in the case of a major disruption. The public-private partnership necessary to accomplish DHS's goals in securing computer networks continues to remain a public-private divide.

I am grieved to note that our Nation's security from a cyber-based attack has not improved since we were here last year. The objective of today's hearing is to highlight immediate steps that DHS and the private sector can take to formalize a partnership

and to ensure effective response and recovery to major cyber network disruptions.

Our economy and national security are reliant on the Nation's information and communications infrastructure, including the Internet. The Internet connects millions of information technology systems and networks together, which, in sum, provide e-commerce to the country and critical services allowing the government to function. On July 19, 2005, we learned that these computer networks can also control physical infrastructure, such as electrical transformers, chemical systems, and pipelines.

DHS recently released its National Infrastructure Protection Plan (NIPP), 3 years after its due date. This plan highlights the importance of cyber security and the Internet to critical infrastructure, stating that the U.S. economy and national security are highly dependent upon the global cyber infrastructure. But according to today's GAO report, DHS fails to adequately plan for recovery of key Internet functions. Moreover, the Department has not adequately prepared to effectively coordinate public-private plans for reconstitution from a cyber Internet disruption.

The success of the protection efforts in the NIPP hinges on information sharing between the Federal Government and the private sector. However, a number of barriers exist to information sharing. Recent incidents at the Department of Veterans Affairs, Department of State, and a national laboratory indicate that the government has trouble protecting sensitive information. The government also does not have a good record of sharing sensitive intelligence-derived threat data with the private sector.

GAO identified numerous challenges to development of a plan and is here today to present the recommendations to strengthen the Department's abilities. Government agencies and private companies, including telecommunications companies, cable companies, peering organizations, and major data carriers, need clarity on what is expected of them in a crisis. Overlapping and unclear roles and responsibilities lead to frustration and confusion, and will hamper recovery efforts in a crisis, which will be deeply injurious to our Nation.

The overarching concern for the Committee is whether the Department of Homeland Security knows what functions of government need to be protected, how those functions interact with State and local governments, and what is DHS's role and responsibility in working with the private sector during a cyber or telecommunication-based incidence of national significance.

The recently released DHS plan requires the use of a risk assessment method that has been criticized as not focusing on what really needs to be protected in the information technology and telecommunication sectors, and focusing heavily on physical assets. The risk assessment methodology should be reevaluated, as it could lead to significant wasteful spending.

While this sector has physical assets to protect, government needs to understand that this sector is about protecting critical functionality, not assets. The private sector and government must work together to ensure the Nation's critical infrastructure can function in the reliable and stable fashion that the American public expects.

Therefore, private industry must devise plans in coordination with the government to ensure critical functions do not fail or can be recovered quickly when faced with an incident of national significance. The National Communications System has worked under this concept for years.

Both government and private industry admit there are vulnerabilities in the networks that can and have been exploited or damaged by accident or natural causes. A perfect system cannot be built. We realize that. The difficult part of any organization, especially government, is how does it respond, recover, and reconstitute after an incident.

The Homeland Security Act of 2002 and Presidential Directives lay out a clear mandate on cyber security at the Department of Homeland Security. They require DHS to assess our vulnerability to a cyber attack, develop a plan to fix it, and implement that plan using measurable goals and milestones. In order to implement the plan, the Department has the admittedly difficult task of engaging and securing action from diverse players, which include State and local governments, other Federal agencies, and especially and most importantly, key industry actors.

The nature of terrorists is to attack private citizens, as we recently saw in the horrific railway attacks in India. There can be no excuse for not effectively engaging the private sector, even though it is hard. We ask no less of our food safety, airline safety, and pharmaceutical industries. The issue is lack of leadership and lack of courage.

Nobody wants to micromanage the private sector or DHS. However, America does expect the Department of Homeland Security and the private sector to take every reasonable measure to protect us from terrorism. I am not convinced that threshold has been met.

If America is to be safe from the damage of a cyber attack, we will need a plan, a budget tied to that plan, and Congressional commitment to the implementation of the plan. One year ago, the Department announced the creation of the position of Assistant Secretary for Cyber and Telecommunications Security to elevate the importance of cyber critical infrastructure protection. Today, this position remains vacant. This vacant post was designed by the Department to lead the Nation in buttressing our critical information technology and telecommunications systems against threats. The Department, working in conjunction with the private sector, needs to find that person and set that person to the task of reforming the plan and then implementing it. A leader can and will be found, and I am encouraging DHS to exhaust every effort to fill this position, ensure the proper authorities are in place to succeed, and ensure that this person receives adequate support from the top leadership at DHS to fulfill the mission.

To that end, I look forward to hearing from our witnesses, NSA, DHS, OMB, GAO, AT&T, VeriSign, and Internet Security Systems, as well as the Business Roundtable. I welcome each of you.

The Department of Homeland Security's testimony came in late last night. It is unavailable to me, the Chairman of this Subcommittee. It will not be accepted as part of it and it is a message to anybody else that wants to play games with the Subcommittee. You are going to send us the information that you want to testify

about on a timely basis so we can do our job. And this is an example of exactly what is happening at DHS on cyber security. You can't meet the goals. You can't meet the expectations. This Subcommittee hearing was noticed June 12—6½ weeks ago, and for the testimony to come in last night is unacceptable and it will not be accepted.

Let me welcome our guests. First is the Hon. George Foresman. He was first confirmed by the U.S. Senate on December 18, 2005. He is responsible for synchronizing national preparedness efforts under the direction of Homeland Security Secretary Michael Chertoff and Deputy Secretary Michael Jackson. He previously served in the Commonwealth of Virginia as Assistant to the Governor for the Commonwealth Preparedness and Homeland Security Advisor, a cabinet-level position. In this capacity, he was the principal advisor and overall coordinator for homeland security and preparedness efforts, as well as relations with military commands and installations throughout the Commonwealth. He is nationally recognized in the fields of emergency preparedness and homeland security.

Richard Schaeffer is the Information Assurance Director at the National Security Agency (NSA). He is responsible for the Information Assurance Directorate at that agency. The Directorate's mission is to provide products and services critical to protecting our Nation's critical information and information systems. Moreover, he is responsible for defining and implementing the information assurance strategy to protect the Department of Defense's global information grid and supporting the ongoing military operations against terrorism.

Next is the Hon. Karen Evans. She is Administrator of E-Government and Information Technology (IT), Office of Management and Budget. She is here as a break from her vacation. I want to tell you how much I appreciate you doing that. She oversees the implementation of IT throughout the Federal Government, including advising the Director on the performance of IT investments, overseeing the development of enterprise architectures within and across those agencies, directing the activities of the Chief Information Officer Council, and overseeing the usage of E-Government funds to support interagency partnerships and innovation. She also has responsibilities in the areas of capital planning and investment control, information security, privacy, accessibility of IT for persons with disabilities, and access to, dissemination of, and preservation of government information.

Next is Keith Rhodes, Chief Technologist, Government Accountability Office (GAO). Mr. Rhodes is currently the Chief Technologist at GAO and Director of the Center for Technology and Engineering. He has been the senior advisor on a range of assignments covering continuity of government and operations, export control, computer security, privacy, e-commerce, E-Government, voting systems, and various unconventional weapons systems. Before joining GAO, he was supervisory scientist leading weapons and intelligence programs at the Lawrence Livermore National Laboratory.

I would like to recognize each of you. Thank you for taking the time to be here. Mr. Foresman, you are recognized for 5 minutes.

**TESTIMONY OF GEORGE FORESMAN,¹ UNDER SECRETARY
FOR PREPAREDNESS, U.S. DEPARTMENT OF HOMELAND SE-
CURITY**

Mr. FORESMAN. Mr. Chairman, thank you, and thank you for the opportunity to appear today to discuss the recovery and the reconstitution of critical cyber networks. Congressional discussion on this particular topic is absolutely essential and it is critical to the success that we need to achieve as a Nation toward strengthening our levels of preparedness.

Mr. Chairman, I would like to highlight several key issues today and outline the Department's roadmap for success in advance of a very important discussion on the security and the protection of our cyber communications networks.

The findings of the GAO report on the development of a joint public-private plan for recovering critical cyber infrastructure and the recent Business Roundtable's recommendations for strengthening cyber preparedness both echo the overall resounding themes that the Department of Homeland Security is pursuing in its work to lead a national effort to protect America's cyber assets. While these reports offer somewhat differing recommendations on the exact steps that we need to take, the shared national vision further reflects two very important and sometimes overlooked issues.

First, the risk posed to the critical cyber infrastructure is becoming both better and more widely understood, both in the public sector and in the private sector. Second, the importance of mitigating these risks, whether on the individual, corporate, or government level, is also better understood. We know we must be ready for the cyber version of Hurricane Katrina or the September 11 attacks.

Mr. Chairman, let me outline for you the Department's three strategic priorities on the cyber preparedness front. They include, one, preparing for a large-scale cyber disaster; two, working to forge more effective partnerships, as you noted in your opening statement; and three, fostering a culture of preparedness to prevent cyber incidents and mitigate damage when disruptions do, in fact, occur.

Our primary strategic goal as part of our overall risk management approach is to prepare for high-consequence incidents. These would include, for example, a widespread disruption involving the Internet or critical communications infrastructure, whether it originates from an attack or from a natural disaster. The Department has established the Internet Disruption Working Group, the IDWG, to address the resiliency and recovery of Internet functions in the event of a major cyber incident. The IDWG is not examining all individual risks, but rather focusing on nationally significant Internet disruptions in a prioritized fashion. The IDWG is developing not only policy recommendations for cyber response, but also operational proposals and protocols to improve the deployment of Federal resources in the event of such an event and how to ensure coordination with local, State, and private sector partners of these assets.

I am also pleased to share with you that the Department conducted its first national cyber security exercise, Cyber Storm, this

¹The prepared statement of Mr. Foresman appears in the Appendix on page 33.

past February, and this was the largest multinational cross-sector cyber exercise to date and assessed the policies and procedures associated with a cyber-related incident of national significance. The Department will soon be releasing a public exercise report on this effort that will outline findings to help bolster protective measures for potential cyber attacks. I will also note that these lessons, like those of Hurricane Katrina and other incidents, will not sit idle. They will be incorporated into our operations processes under the National Response Plan and these will be retested during Cyber Storm II in 2008, if not before.

Cyber Storm demonstrated the close cooperation and information sharing needs across Federal agencies, across international boundaries, and most importantly, between the public and the private sectors. The exercise tested for the first time the full range of cyber-related response policy, procedures, and communications methods required in a real-world crisis. We know that there were successes. We also know that there is room for improvement.

Another significant accomplishment in preparing for a nationally significant cyber disruption is last month's completion, as you noted, of the National Infrastructure Protection Plan. The NIPP sets forth a comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities for DHS, Federal sector-specific agencies, other Federal, State, local, tribal, and territorial agencies, as well as our private sector security partners. The plan addresses the physical, human, and cyber elements of the critical infrastructure issues which cross all sectors. This release of the NIPP is an important milestone, as it accompanies 17 sector-specific plans that will help build a safer and more secure and more resilient America by enhancing protection of the Nation's critical infrastructure and key resources to include the cyber community.

Our second strategic goal is to improve the Department's partnership programs and practices. Homeland Security Presidential Directive 7, the Administration's policy on critical infrastructure protection, explicitly recognizes the importance of partnerships, which are essential for many sound reasons. In the cyber security arena, the Department is working to nurture existing partnerships and establish new relationships with three key stakeholder communities, the private sector, Federal departments and agencies, and the State, local, and tribal governments, as well as academia.

Third, we must create a culture of preparedness, both to prevent a cyber disaster and to mitigate damages if a widespread disruption occurs. We are working every day to influence how individual citizens, government, and the private sector prepare for the security challenges of the coming decade. As with our other strategic priorities, this goal demands a focused and disciplined approach. We need interconnected strategies and processes, not individual actions. Just as our cyber systems are interconnected, so must be our approach to dealing with disruptions.

Our national cyber security efforts are rapidly maturing and we have clear legislative and presidential direction and private sector interest. There is no magic wand that will allow us to do this overnight. There is, however, a growing coalescing of effort between government and the private sector as just two of the key entities.

Chairman COBURN. I need for you to summarize, if you will.

Mr. FORESMAN. Yes, sir, and I am finishing up. To create a long-term culture of preparedness, we are developing clear organizational doctrine which memorializes strategic policies, clarifies roles and responsibilities, and defines measures of accountability. The road ahead is critical and we are committed to ensuring success. Thank you.

Chairman COBURN. Thank you. Mr. Schaeffer.

TESTIMONY OF RICHARD C. SCHAEFFER, JR.,¹ DIRECTOR OF INFORMATION ASSURANCE, NATIONAL SECURITY AGENCY

Mr. SCHAEFFER. Good morning, Mr. Chairman.

Chairman COBURN. Good morning.

Mr. SCHAEFFER. I appreciate the opportunity to be here today to talk briefly about the NSA's information assurance mission and its relationship to the work of the Department of Homeland Security and others concerned with helping operators of crucial information systems prepare for and recover from hostile acts or other disruptive events.

The NSA's information assurance mission focuses on protecting what National Security Directive 42 defines as national security information systems, systems that handle classified information or are otherwise critical to military or intelligence activities.

Historically, most of our work has been sponsored by and tailored for the Department of Defense. Today, national security systems very often rely on commercial products or infrastructure or interconnect with systems that do. This creates significant common ground between defense and broader U.S. Government and homeland security needs. More and more, we find that protecting national security systems demands teaming with public and private institutions to raise the information assurance level of products and services more broadly. If done correctly, this is a win-win situation that benefits the whole spectrum of information technology users, from warfighters and policy makers to Federal, State, local governments and operators of critical infrastructure and major arteries of commerce.

This convergence of interests has been underway for some time and we can already point to several examples of the kind of fruitful collaboration it inspires. For instance, the NSA and the National Institute of Standards and Technology have been working together for several years to characterize cyber vulnerabilities, threats and countermeasures to provide practical cryptographic and cyber security guidance to both IT suppliers and consumers.

Among other things, we have compiled and published security checklists that harden computers against a variety of threats. We have shaped and promoted standards that enable information about computer vulnerabilities to be more easily cataloged and exchanged, and ultimately, the vulnerabilities themselves to be automatically patched. And we have begun studying how to extend our joint vulnerability management effort to directly support compliance programs, such as those associated with the Federal Information Security Management Act. All of this is unclassified and ad-

¹ The prepared statement of Mr. Schaeffer appears in the Appendix on page 50.

vances of cyber security in general, from national security and other government networks to critical infrastructure and other commercial and private systems.

The NSA partners similarly with the Department of Homeland Security. In 2004, DHS joined the NSA in sponsoring the National Centers of Academic Excellence Program to foster training and education programs to support the Nation's cyber security needs and increase the efficiency of other Federal cyber security programs. The NSA has supplied trained personnel and other technical support to the U.S. Computer Emergency Readiness Team, and we routinely alert one another to possible or emerging hostile cyber threats. In fact, DHS has just named an integree to work in the NSA-Central Security Service Threat Operations Center, which has as one of its missions to monitor the operations of the global network in real time to identify network-based threats to DOD and intelligence community networks.

NSA and DHS cooperate on investigations and forensic analysis of cyber events and malicious software, and together, we look for and mitigate the vulnerabilities in various technologies that would render them susceptible to similar attacks. We each bring to these efforts complementary experience, insight, and expertise based on the different problem sets and user communities on which we concentrate, and we each then carry back to those communities the dividends of our combined wisdom and resources.

With regard to post-incident response, the NSA supplies technical personnel, advice, and equipment to support an efficient response and recovery to disasters. The NSA has worked with the DHS Infrastructure Protection Division to plan for interoperable communications systems needed to support response and recovery. We did this for Hurricane Katrina and do it for other disasters, as well.

When it comes to reconstructing networks, however, beyond just communications systems, bringing in replacement technology may be the easy part. The real challenge is knowing what to reconstruct. That means maintaining an up-to-date understanding of what set of data, functions, and connections available to what set of users qualify as critical.

Looking forward, NSA and DHS interests will continue to merge and the opportunities needed for shared network and mutual support will continue to grow.

Finally, beyond technical convergence, in the post-September 11 world, the NSA and DHS are bound together by the need to provide for communications across once unbridgeable chasms of classification and practice, from the President all the way to first responders and the owners and operators of critical infrastructure. As a starting point, the NSA and NIST have established a suite of unclassified algorithms that can be implemented in commercial off-the-shelf offerings as well as specialized high-end government equipment. This sets the stage for interoperable encryption and message authentication and is an important step, although just one step in the broader effort to ensure that the Nation can recognize and respond to impending emergencies or their aftermath.

Once again, thank you, Mr. Chairman, for giving me the opportunity to appear before you today and for your leadership in this area.

Chairman COBURN. Thank you, Mr. Schaeffer.

Next, Ms. Evans, just a side note. Thanks for all your help on our Government Accountability and Transparency Act. It passed the Committee unanimously yesterday.

TESTIMONY OF KAREN EVANS,¹ ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

Ms. EVANS. Congratulations. Good morning, Mr. Chairman, and thank you for inviting me to speak about “Cyber Security: Recovery and Reconstitution of Critical Networks.” My testimony today will focus on OMB’s activities to improve security and resilience of the Federal Government’s cyber critical assets.

Last year, the Director of OMB issued a regulation on maintaining telecommunication services during a crisis or an emergency. The regulation required each agency to review its telecommunications capability in the context of planning for contingencies and continuity of operation situations. OMB also asked each agency to confirm that they were complying with directives issued by the National Communications System (NCS), and guidance issued by the Federal Emergency Management Agency (FEMA).

In August 2005, all large agencies submitted reports on the status of their telecommunications services. OMB and the NCS analysis revealed the need for additional guidance to the agencies regarding the use of redundant and physically separate telecommunications service entry points into buildings and the use of physically diverse local network facilities.

In October 2005, the NCS hosted a Route Diversity Forum for representatives from over 70 Federal agencies. In addition, the NCS developed a Route Diversity Methodology, enabling agencies to self-assess their own facilities.

When an agency initiates new telecommunications procurements, the agency must determine the appropriate level of availability, performance, and restoration that is required. The General Service Administration’s upcoming Networx procurement will specify telecommunications infrastructure security requirements to protect contract network services, infrastructures, and information processing resources against cyber and physical threats, attacks, or system failures. The Networx program will ensure that telecommunications capabilities are continuously ready to meet the needs of the Federal agencies during national emergencies.

On December 17, 2003, the President signed Homeland Security Presidential Directive 7, “Critical Infrastructure Identification, Prioritization, and Protection.” This directive established the national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and to protect it from terrorist attacks. OMB worked with the Department of Homeland Security to evaluate the protection plans. We have provided each agency

¹The prepared statement of Ms. Evans with an attachment appears in the Appendix on page 53.

with a written response explaining our approval, our disapproval of the agency's cyber security plan, and highlighting areas where improvements were needed.

Additionally, each year, agency CIOs, chief information officers, and program officials conduct IT security reviews for systems that support their programs. As part of their evaluations, agencies are asked to categorize their information systems into high, moderate, and low impact and document the security controls implemented for each.

Last, the National Cyber Response Coordination Group is the principal Federal interagency mechanism to coordinate the preparation for and response to cyber incidences of national significance. OMB is a member of the group, along with other agencies having a statutory role in cyber security, cyber crime, or protection of critical infrastructure. During a cyber incident, the member agencies would integrate their capabilities in order to assess the scope and severity of the incident, govern response and remediation efforts, and advise senior policy makers. The group would also use their established relationships with the private sector and State and local governments to help manage the cyber crisis and develop recovery strategies.

In conclusion, each agency is responsible for ensuring the continued availability of its mission-essential services. Strategic improvements in security and continuity of operations planning can make it more difficult for attacks to succeed and can lessen the impact of attacks when they occur. The Administration will continue to work with the agencies, Congress, and GAO to ensure appropriate risk-based and cost-effective IT security programs, policies, procedures are put in place to protect the Federal Government's critical cyber infrastructure.

I would be happy to take any questions, sir, that you may have.
Chairman COBURN. Thank you, Ms. Evans. Mr. Rhodes.

**TESTIMONY OF KEITH RHODES,¹ CHIEF TECHNOLOGIST AND
DIRECTOR, CENTER FOR TECHNOLOGY AND ENGINEERING,
U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. RHODES. Thank you, Mr. Chairman. We appreciate the opportunity to testify on our Internet reconstitution report being released today that we completed at your request.

Last summer when GAO testified before your Subcommittee, we discussed the work that remained for DHS to fulfil its cyber security responsibilities in 13 key areas, including developing a plan for recovering the Internet when it is disrupted. Despite Federal policy requiring DHS to develop this integrated public-private plan, to date, no such plan exists.

Today, at your request, we will briefly discuss the growing threats to the Internet, where our Nation is in its efforts to develop this plan, and recommendations to both DHS and the Congress to facilitate public and private efforts to recover the Internet when major disruptions occur.

First, threats. Criminal groups, foreign intelligence services, hackers, and terrorists are all threats to our Nation's computers

¹ The prepared statement of Mr. Rhodes appears in the Appendix on page 111.

and networks. A recent intelligence report on global trends forecasts that terrorists may develop capabilities to conduct both cyber and physical attacks against infrastructure nodes, including the Internet. In fact, the Internet itself has been targeted and attacked and private companies who own the majority of the Internet infrastructure deal with cyber and physical disruptions on a regular basis.

For example, viruses and worms are often used to launch “denial of service” attacks that result in traffic being slowed or stopped. Several recent cyber attacks highlight the importance of having robust Internet recovery plans, including a 2002 coordinated denial of service attack that targeted all 13 Internet route servers.

For most of these attacks, the government did not have a role in recovering the Internet, but recent physical attacks like the terrorist attacks of September 11, 2001, and Hurricane Katrina, highlight the need for public-private coordination associated with Internet recovery. DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated public-private plan, but these efforts are not yet complete nor are they comprehensive.

Specifically, DHS has developed high-level plans for infrastructure protection and national disaster response, but components of these plans that are to address Internet recovery are incomplete and inadequate. For example, the National Response Plan Cyber Annex does not reflect the National Cyber Response Coordination Group’s current operating procedures. DHS has started a variety of initiatives to tackle this problem, including working groups to facilitate response and exercises to practice recovery efforts. However, these efforts are immature and the relationships among groups like the Internet Disruption Working Group and others are not evident.

Regarding challenges that have impeded progress, first, it is unclear what government entity is in charge, what the government’s role should be, and when it should get involved. Expanding on each of these, DHS National Cyber Security Division and the National Communications System have overlapping responsibilities. In addition, there is a lack of consensus about the role DHS should play. The government is pursuing the grandiose plan approach with the NIPP and the National Response Plan, while the private sector wants more of an assist or tactical role from the government than our report lays out in detail. And triggers that clarify when the Federal Government should be involved are unclear.

Second, our Nation is working in a legal framework that doesn’t specifically address the government’s roles and responsibilities in the event of an Internet disruption. In addition, the Hurricane Katrina recovery effort showed that the Stafford Act can create a roadblock when for-profit companies that own and operate critical infrastructures need Federal assistance during national emergencies.

Third, the private sector is reluctant to share information with DHS because it does not always see value in sharing, does not necessarily trust the government, and views DHS as an organization lacking effective leadership.

To address these inadequacies, our statement includes nine specific recommendations for DHS, including determining who should

be in charge given the convergence of voice and data communications, developing a plan that is consistent with what the private sector infrastructure owners need during a time of crisis, and incorporating lessons learned from incidences and exercises.

In addition, the Congress should consider clarifying the legal framework that guides roles and responsibilities for Internet recovery.

In summary, Dr. Coburn, exercises to date and a recently issued report by the Business Roundtable found that both the government and private sector are poorly prepared to effectively respond to cyber events. Although DHS has various initiatives underway, these need to be better coordinated and driven to closure. Until that happens, the credibility of the Department will not be where it needs to be to build effective public-private relationships needed to effectively respond to major Internet disruptions.

This concludes our statement. Thank you, Mr. Chairman, and we are prepared to answer any questions the Subcommittee may have.

Chairman COBURN. Thank you very much.

Mr. FORESMAN, your response to Mr. Rhodes' report?

Mr. FORESMAN. Mr. Chairman, let me offer two responses. One, as we have gone through that report, we clearly agree that the road ahead, whether we are talking about GAO or the private sector, we agree on the road ahead.

I would, however, not agree with him in terms of the perception that he might leave in the relationship with the private sector. My fourth day on the job back in January, one of the first groups I met with in this particular case was the Business Roundtable and one of the key issues we talked about were cyber security, the concern about reconstitution and recovery of the Internet, and I think that as you said in your statement, Mr. Chairman, this is not easy and there are a lot of folks who have said, well, it is not where it should be, and I would agree. But we need to have definitive milestones. We need to have definitive deliverables.

But I will tell you, sir, just as your comment to us that we need to work closely with the private sector, getting agreement across the various elements in the private sector, whether it is the information technology sector or the telecommunications sector, this is not easy. We are not in a position to force them. We are coalescing the road ahead.

So I would agree that we share the vision. I think his assessment in terms of progress is much bleaker than what is the actual progress to date.

Chairman COBURN. Why would the private sector be reluctant to give DHS information on this?

Mr. FORESMAN. Mr. Chairman, I think there are three things. There are those elements of the private sector that are reluctant to give us information and there are those elements of the private sector that are not reluctant to give us information. A conversation with a handful of people does not, I think, effectively reflect the private sector as a whole because the private sector is rapidly big.

But as you know, there are a couple of issues here. One, there is the concern of our private sector partners out there, the proprietary nature of the information that they have in a business competitive environment. They want further and stronger assurances

that proprietary information is not going to be shared with competitors.

The second issue, and frankly is a legitimate issue, is government and the private sector have typically operated in a regulator-regulatee relationship over the past 20 or 25 years. When we talk about the IT community, it is not, if you will, regulated by government, and clearly there are the institutional—

Chairman COBURN. Thank goodness.

Mr. FORESMAN. Yes, sir, and clearly, the institutional barriers to getting beyond a 25- or a 50-year culture to get into a collaborative partnership is not a culture that you change overnight. And so I think it is part policy, it is part culture, but we are seeing more and more every day as we collaborate with the private sector. As our US-CERT, for instance, gets specific information provided to us through a variety of sources, such as the NSA, we rapidly get that information out to the private sector and they rapidly come back to us with information. So it sometimes comes down to who did you talk to last and what is it that they said to you?

Chairman COBURN. Well, the group that I talked to last were the ISPs and the telecommunications companies, and I would tell you in that meeting, uniformly, there was no trust of DHS with any of their proprietary data, and that was in a classified briefing I had 3 months ago. How do you establish the leadership role and the trust that allows the private sector to do what they know how to do that you don't know how to do?

Mr. FORESMAN. Well, Mr. Chairman, this comes down to the continued interaction. As Ms. Evans identified and as other folks have identified, we have got a number of working groups where we have got government and the private sector sitting side by side, developing sector-specific plans, for instance, under the National Infrastructure Protection Plan, and trust is not a function of me coming into the room and sitting with our private sector partners and saying, trust me. We have to prove it.

This is the benefit of these joint planning activities. As much as we would like them to be done in immediacy overnight, they are not. But just as it is taking time to develop those plans, one of the important byproducts is that we are raising trust every day when we put these people in the room together.

Chairman COBURN. I will be submitting some questions to you separate from that. I would hope that we could get a timely response.

Mr. FORESMAN. Mr. Chairman, I will ensure that you get a timely response and I will acknowledge that we were remiss in not hitting the deadline on getting our testimony to you. I accept full responsibility and I will give you my personal assurance that we will correct those issues in the future.

But I also want to underscore, by no means were we trying to not get information to you. This is a critically important area. This Subcommittee is one of the few committees across the Congress that has shown a continuing interest in this area. It is not an easily understood area, and frankly, this level and more of this type of dialogue is going to be absolutely critical to our success.

Chairman COBURN. Mr. Schaeffer, at NSA, tell me about your relationship with the private sector and trust and relationship and

information sharing and how have you developed that and how do you utilize that. Have you emphasized recovery more than physical asset protection?

Mr. SCHAEFFER. Well, sir, I think our relationship with industry or the private sector is on a number of levels. Clearly, there are, as I mentioned in my testimony and others did, as well, the dependence upon the private sector to deliver the technology, the capabilities that we need within the national security community, and quite frankly, across the entire Nation, is dependent upon the reliability, the security of that technology. So we have a very deep relationship with the private sector in establishing on a one-on-one basis the availability of vulnerability information of the products that they provide, assisting them in increasing the overall security or assurance of those products, and then we also work with the infrastructure providers themselves to understand the vulnerabilities within those environments and help them address the situation, the improvements that can be made in that environment.

Most of our relationships that are strong come from a one-on-one basis with the agency. We participate. We collaborate with industry associations and do that in a very open and, I think, positive way. But I think as Mr. Foresman outlined, it is a situation that takes a tremendous amount of work with individual companies, then with industry or association groups, and then in larger forums to build the trust and confidence that information that is exchanged with the government, and in this case NSA, receives the appropriate level of protection. It is something that we work on every day. It takes that sort of attention and commitment.

And we have seen actually tremendous progress over the last several years as the community at large, the public-private community, has come to better understand the risks associated with operating in this highly networked environment and the need for close collaboration amongst public-private enterprises to better understand the vulnerabilities and ways of mitigating them.

I think we are an example of where it has worked because we have developed the trust and confidence over a long period of time with companies, trade groups, industry associations, and so forth, and I see promise in what DHS is leading, in what DHS is participating in, and quite frankly, what I see the entire IT industry participating in. We are just at the bottom of a very steep hill.

Chairman COBURN. Has NSA's main focus been on functionality?

Mr. SCHAEFFER. No, sir. NSA's main focus has been on the assurance of the functionality that is provided in the devices, so—

Chairman COBURN. That is what I mean. But the goal is function. The ultimate goal for security is to maintain function, or to recover function.

Mr. SCHAEFFER. Yes, sir. That is correct.

Chairman COBURN. All right. Mr. Rhodes, you mentioned the working groups aren't communicating. We don't have cross-reference. You also mentioned a role that is more grandiose rather than recovery. Talk for a minute, if you would, about the working groups that have been established and what you see that needs to be changed there so that we accomplish this goal of protecting and recovering functionality.

Mr. RHODES. The big struggle with the working groups seems to be that there are a lack of roles and responsibilities and clear lines of authority. There seems to be a not clear definition of how the working groups relate to one another—

Chairman COBURN. In other words, they could come up with a really appropriate plan, but have no authority to get that plan implemented?

Mr. RHODES. And no milestones. Your original point about budget against effect, a recommendation with money, a recommendation with schedule, not just—they can come up with that, but then what is their schedule? What is their time line? What is their relationship? That is the main struggle we see.

Also, working groups without authority. What purpose do they serve? If they don't—if no one has the hammer, if no one has the authority to get anyone to do anything, then it is just another group that meets to meet instead of meeting to get something done. As you say, they could have very fine recommendations, but where do they go from there?

Chairman COBURN. OK. One last question for you, the comment on the Stafford Act. I don't believe we have gotten anything, and I may be wrong, from the Administration on modifying the Stafford Act so that we can help the telecommunications industry and the Internet industry to recover by assisting them with either protection or transportation or security as they bring these systems back up. Would you agree that is something that we ought to hear from the Administration? And we may have, I am just not aware of it.

Mr. RHODES. We haven't seen anything, either, but when you look at the tactical needs, the tactical view that private industry takes, they are talking about just those things—fuel, access, transportation. They are not talking about, tell me how to bring the Internet back up. They are saying, let me get into the disaster area with my business credential or some emergency credential issued by the U.S. Government so I can go to the location to do the job that the government can't.

Chairman COBURN. And modify the law so that the government assets—

Mr. RHODES. And modify the law—

Chairman COBURN [continuing]. And assist that effort.

Mr. RHODES. Absolutely. I mean, what we hear from private—and it is not just relative to the Internet, it is whether we are talking to the chemical industry or we are talking to gas and oil or we are talking about the power grid or folks like that, they are all saying, let me do my job. I am not the enemy because I am for profit.

Chairman COBURN. Yes.

Mr. RHODES. I am the infrastructure. Let me go into the area I am supposed to in order to fix it.

Chairman COBURN. Right. Which we saw lots of problems with during Hurricane Katrina.

Mr. RHODES. Absolutely, and saw it during September 11, 2001, also.

Chairman COBURN. All right. Ms. Evans, not long ago, the Federal Government's critical infrastructure protection coordination efforts were run out of the White House and some in private sector viewed this, and I think probably still do, as a higher Administra-

tion priority than it is now. Should these initiatives remain within DHS or should we consider the prior model?

Ms. EVANS. The model that we have right now is in place as a follow-on from the Homeland Security Act as well as the President's HSPD-7, which clearly outlines that the Secretary of Homeland Security has the responsibilities for these activities. This does not mean that the Administration does not view this as a priority, because oversight activities still occur out of the White House and the Executive Office of the President, with the Office of Management and Budget, myself, as well as the Homeland Security Council. So the Administration is very much committed to this and continues to have cyber security reconstitution, continuity of operations, as a priority.

I do think that the model that we have in place right now is an effective model and can work, because the actual work and execution happens in the agencies. The President holds the Secretary accountable for these actions. The President holds him accountable for getting these plans in place with clear milestones. This clearly has been talked about, and to achieve the results.

We, in the White House, do not do the actual execution. The work is done out in the agencies. And so it doesn't diminish that the Administration doesn't view this as a priority by having a person clearly responsible for the execution of these activities at a department level.

Chairman COBURN. Any of you can respond to this if you want. It just seems to me that 75 percent of this is private sector. Why wouldn't the Administration's view say, OK, you are the guys that know all this. You are the guys who are responsible for it. Your bottom line depends on it staying up and working. Why don't you go tell us what you think we ought to do rather than us tell you what we think you ought to do? Why shouldn't the debate be, private industry, come tell us what to do. Why shouldn't the organizational framework be, let us listen to them and then let us create the framework based on what they suggest we ought to do rather than top-down? Why not private industry up?

Mr. FORESMAN. Mr. Chairman, if I might, that is exactly what we are doing, and that is why we have the National Infrastructure Protection Plan. That is why we have the development through the sector coordinating councils. The role of the Federal Government is not to tell the private sector what to do. It is to create the environment to provide for a national approach, and what I mean by that is the Federal Government is uniquely positioned to bring together the elements of local government, State government, tribal and territorial, the private sector partners, because this is a homeland security issue. It is a national security issue.

So our job is to get all of the players around the table and to go through and get the best and the brightest in the room to say, what is it that we, as a Nation, need to be doing, because this is not a Federal issue. It is clearly a national issue.

Chairman COBURN. Do you think that is happening right now?

Mr. FORESMAN. Senator, I don't think it is happening to the degree that it should, and I think, as all of the folks have pointed out, this continues to be a growth effort, a growing effort on the part of this Nation in the post-September 11 era. When I was vice

chairing the Gilmore Commission prior to September 11, we raised the whole issue of critical infrastructure protection and the fact that a significant amount of work needed to be done. I don't think we have reached the optimal level of private sector direction and input into it, but at the end of the day, I don't think we were going to start—we are not going to start at the perfect position. This is very much a learning process for everyone, Federal, State, local, public sector, and private sector.

Chairman COBURN. Well, the private sector is being attacked all the time now and they are responding, both in terms of physical assets and software and encryption and everything else. They are doing the things because they are seeing the attacks anyway. It just seems to me we have got it backwards. We ought to have the private sector come together and say, here is how we think you ought to mobilize State and local governments. Here is how we think you ought to set up the structure to best maintain this. Here is how we think you assure protection.

What would happen to this economy if you had a 4-week disruption, interruption of the Internet? We would be on our back, and everybody knows that, and yet the urgency to make sure that can't happen, or if it did happen to recover quickly, I don't see anywhere except in the private sector.

Mr. FORESMAN. Mr. Chairman, I would respectfully disagree in this context. We are aware of a variety of things we obviously cannot get into in an open hearing—

Chairman COBURN. I understand that.

Mr. FORESMAN [continuing]. But we are aware of a significant number of things that have occurred in recent time that the private sector was not aware of had government not made them aware of it. So we are doing our part to give them the information. They, in turn, are assessing the situation, bringing recommended solution sets back to us, implementing solution sets in the broadest of terms, and so our role wasn't to go to them and say, here is the problem. Here is what we want you to do to fix it. We made them aware of the problem. We know that they are the owners and the providers of a lot of the critical IT backbone. They assessed it. They took steps. And this happens hundreds, if not thousands, of times every month. I would very much underscore that US-CERT, as just one example, there is daily ongoing dialogue between Federal agencies and the private sector, not in the context of here is what you have to do, but here is the problem and please come back to us.

Now, I will tell you that there are going to be times that the private sector is going to assess the risk differently than we do in government and then they are forced to make a business decision about whether they are going to invest the time and effort into it to address it. So this is all part of the trust process that we can get to an equal common ground.

Chairman COBURN. Fair enough. One last question for Ms. Evans, and I will have questions for each of you. I also would like for you to have staff stick around here to hear our other panelists because routinely I see Administration witnesses leave before those that have a different position and constructive criticism can be heard.

Ms. Evans, do you have enough staff to handle the cyber security of critical infrastructure and Federal information security management?

Ms. EVANS. My answer would be yes, sir, that I do. We have subject matter experts for each of the areas that I am responsible for and the way that we manage within OMB is that we have portfolios of agencies and we work very closely with all parts of OMB so that we are managing the issues across the board as they affect each of the agencies. So it isn't just my staff, but it is the entire resources that are available within OMB because we take a portfolio approach to this.

There is one thing that I would like to follow up on, Mr. Foresman's comment, and this is what the government is doing as a whole, at least from a Federal perspective. We do view it as we are buying services, because we don't own the infrastructure. There are activities that we have done and that we are continuing to do. In my written testimony, I have included the information security line of business.

But as you know, we spend \$65 billion on information technology, so in the course of that spending, we make it very clear what the services are that we need, what the risk is associated with the services and the information we need to protect, and as Mr. Foresman said, then it is up to industry to offer us the solutions back, and the way that we structure those procurements is not to tell them, we want you to do X, Y, and Z, but to really frame, this is the service, this is the recovery level, this is the level of risk that we are willing to accept. Here is the type of protection that we think we need to have. And then we do look to private industry to give us the solutions that can best service those needs, because as you have said, sir, it is about the functionality and the mission critical nature of the services that we provide that we need to have that reliability.

Chairman COBURN. I would like you to repeat that number so everybody can hear what you spend annually on IT.

Ms. EVANS. Sixty-five billion dollars.

Chairman COBURN. This Subcommittee will have a hearing on whether or not that is spent properly or not. I can tell you, from the Defense Travel System, you certainly haven't spent the money properly. So we will be looking at that.

Ms. EVANS. Well, we are looking forward to it, yes, sir. [Laughter.]

Chairman COBURN. Sixty-five billion dollars is a lot of IT.

Thank you. You will each receive questions. Thank you for the report from GAO. I thank each of you for your service to our country and I would dismiss this panel and ask our next panel to come forward.

I am going to start introducing our witnesses while they are being seated. Thomas Noonan is Chairman, President, and Chief Executive Officer for Internet Security Systems (ISS). He is responsible for the overall strategic direction, growth, and management of the company. Under his leadership, ISS revenues soared from start-up in 1994 to nearly \$330 million in its first decade. The company has grown to more than 1,200 employees with operations in 26 countries. In 2002, President Bush appointed Mr. Noonan to

serve on the National Infrastructure Advisory Council, a homeland defense initiative that protects information systems that are critical to the Nation's infrastructure. He currently chairs the NIAC Evaluation Enhancement of Information Sharing and Analysis Working Group.

Robin Bienfait, Senior Vice President, Global Network Operations, AT&T, welcome. She is the first woman in company history to be responsible for AT&T's global network, including local, data, and voice network worldwide. I pay them a lot of money every month. In addition, she leads teams that manage network security and global network disaster recovery. And additionally, she previously led AT&T's international and domestic core network operations and technical support division and has held a variety of other technical and leadership positions of increasing responsibility since joining AT&T in 1985. She is a graduate of the Georgia Institute of Technology with a Master's degree in management of technology. She also holds a Bachelor's degree in engineering from Central Missouri State University and an Associate in Business degree from Maryland University, European Division.

Michael Aisenberg, Director of Government Relations for VeriSign, serves as the company's principal liaison with the Administration and Federal agencies, including the Departments of Homeland Security, Defense, State, and Justice. He manages a portfolio of policy issues, including global infrastructure security, digital signatures, e-health, intellectual property and government procurement on behalf of the world's leading Internet trust and identity provider. He is the Vice Chairman and Chair-Elect of the Information Technology Sector Coordinating Council. In 2004, he was elected Chairman of the ITAA's Information Security Committee. He leads VeriSign's participation in the President's National Security Telecommunications Advisory Committee. He holds a B.A. from the University of Pennsylvania, a J.D. from the University of Maine Law School. He attended Georgetown University Law Center in 1975 and 1976, and upon graduation served 5 years as an attorney advisory and legislative counsel at the FCC.

Karl Brondell, Strategic Consultant State Farm Insurance Companies, representing the Business Roundtable here today. He is a CPCU, a strategic consultant in the Strategic Resources Department of State Farm Insurance Company. He is the past Chairman of the Board of Directors for the Insurance Placement Facilities of Pennsylvania and Delaware. He is a member of the national CPCU International Insurance Section Committee and an at-large Board of Director for Villanova University's Executive MBIA Alumni Association. He received a Bachelor's degree from Benedictine College, Acheson, Kansas. I, by the way, have visited there. He has a Master's degree from Villanova University in Villanova, Pennsylvania. He earned the Charter Property and Casualty Underwriter Designation and holds an Associate in Claims certificate and a certificate for general insurance.

Welcome to you all. We will start with you, Mr. Noonan.

**TESTIMONY OF THOMAS E. NOONAN,¹ PRESIDENT AND CHIEF
EXECUTIVE OFFICER, INTERNET SECURITY SYSTEMS**

Mr. NOONAN. Mr. Chairman, thank you for the opportunity to appear before you today. My name is Tom Noonan. I am President and Chief Executive Officer of Internet Security Systems. We are a leading provider of preemptive cyber security technologies for large-scale enterprises, and I represent the technology industry today.

We operate five cyber security centers around the world, two in the United States, the rest in Asia through Tokyo, Australia, Brussels, and a partner operation in Latin America. We protect our customers by monitoring the Internet for cyber threats 24 hours a day, 365 days a year, providing preemptive protection for customers. This is critical preemption before reconstitution, obviously. We utilize that security intelligence, technology, and expertise to preempt the strikes that would cripple critical networks and stay ahead of the threats.

I want to stress three important messages about our Nation's security landscape this morning, and this comes from my 13 years in this industry as one of the founders of this company and a person that has been working to advocate better security practices in both the private and public sector.

First, threats to the critical infrastructure are real, and without a doubt, they are growing. The question is not if but when. The explosive growth of new Internet technologies, from wireless to voice-over Internet telephony, has engendered new threats that are far outpacing the security responses of many private and governmental users.

Second, the intelligence protocols and technologies necessary to protect against emerging cyber threats are, by and large, robust and widely available. In other words, we have the tools at our disposal today to safeguard our critical infrastructure.

And finally, despite our knowledge of these threats and our overall ability to protect ourselves, we as a Nation are not doing nearly enough to preempt the types of attacks that could debilitate our critical network infrastructure. Leadership is desperately needed at the Federal level, not to replicate existing private sector efforts but rather to extend the impact of those efforts by encouraging the private sector to collectively increase in cooperation with the government.

This means five things for me this morning. First, appointing an Assistant Secretary of Homeland Security for Cyber Security and Telecommunications who will help secure the Federal Government's own networks as well as those of the broader economy.

Second, clearly delineating and hardening the roles and responsibilities of many public-private entities working today to secure cyberspace.

Three, ensuring that the Federal Government makes use of existing industry resources to gather and analyze data on cyber security threats and methods.

Four, creating a national plan to restore connectivity on a prioritized basis.

¹ The prepared statement of Mr. Noonan appears in the Appendix on page 132.

And five, providing sustained Federal funding—that \$65 billion sounds like a lot, but sustained Federal funding and active Congressional oversight to ensure that the Department of Homeland Security is getting the job done for this country.

I think we know cyber threats are serious and they are growing in sophistication. The rules of criminal hacking today are no longer shaped by teenage malfeasants, but by confederated crime operations that are driven by the economics of opportunity, incentive, and risk, just like traditional theft, burglary, and extortion.

I think it is this professionalization of cyber crime that is unsettling for many reasons, not the least of which are indications that those who would seek to do harm to our Nation have been working to improve their technological abilities. Particularly unsettling is not just the threat to privacy information, which we read about in the newspaper, or our e-commerce applications, but more importantly to the very control networks of the automated systems that control and regulate our Nation's industrial systems, like SCADA. Control systems are now Internet-connected and they are susceptible to major attacks. Under contract with customers, ISS has conducted real world penetration tests with large power plants and others to show that they are at risk.

Put simply, Mr. Chairman, the fact that our Nation's critical infrastructure has yet to fall victim to a significant and coordinated cyber attack does not mean that it can't happen. Emerging technologies coupled with an exponential increase in the use of new applications on the Internet have opened many new avenues to attack and keeping up with this large increase in vulnerabilities is a daunting task. It is only complicated by the shrinking window that we are seeing between the time a vulnerability is disclosed and the time that it is exploited by criminal interests.

I think there is good news, Mr. Chairman. Our Nation already has the technological capabilities to protect the critical infrastructure. Private industry is operating positively against many of the requirements associated with technology, vulnerability, discussion, etc. But what is missing is genuine leadership on the part of the Federal Government. We, as a Nation, can protect our critical infrastructure, and in fact, we already are, but that requires also Federal leadership.

I think your role here boils down to two things. The first one is minding the store, and I know that Secretary Chertoff and the Department of Homeland Security are working around the clock to protect the Nation, but we need to be able to talk to the person who is minding the store and that is the Assistant Secretary.

Second, it is difficult for the Federal Government to preach strong cyber security practices across our economy when the Federal networks themselves are so woefully unprotected. While steps have been taken in recent years to improve agency security practices through FISMA, most Federal agencies are still getting failing marks when it comes to securing their networks.

When it comes to strengthening Federal leadership, I just want to reiterate these five points in closing. Appointment of the Assistant Secretary for Cyber Security and Telecommunications. The job has been open for over a year.

Two, a clear delineation and hardening of the roles and responsibilities of these countless public-private entities.

Three, ensuring that the Federal Government makes full use of existing industry resources. We are absolutely willing and able to participate as a private sector.

Four, we need to develop the national plan to restore connectivity on a prioritized basis.

And five, sustained Federal funding.

So there is no silver bullet here, Mr. Chairman. Securing our Nation's infrastructure from cyber attack requires a heightened degree of public-private coordination and I think it is a challenge but it is one we are up to. We are pleased at ISS to be partnering with you and I thank you for the opportunity to participate this morning.

Chairman COBURN. Thank you. Ms. Bienfait.

**TESTIMONY OF ROBERTA A. BIENFAIT,¹ SENIOR VICE
PRESIDENT, GLOBAL NETWORK OPERATIONS, AT&T**

Ms. BIENFAIT. Good morning, Mr. Chairman.

Chairman COBURN. Good morning.

Ms. BIENFAIT. My name is Robin Bienfait and I am Senior Vice President of AT&T's Global Network Operations. I want to thank you for allowing me to share with you what we have done and what we are generally doing to ensure the reliability and restorability of AT&T network services. We are committed to a strong public-private partnership and we hope our experience is helpful.

We believe there are keys to network security and disaster recovery and I will focus on the following areas: The strength of the public-private partnership; the lessons learned, especially from Hurricane Katrina and the 2003 Midwest and Northeast power outages; and a series of policy recommendations.

Our country relies on cyber and physical infrastructure that is provided by a very close partnership among all the providers and users of this infrastructure. Each partner, both in the public and private sector, has a responsibility to keep their part of the infrastructure working. They also each have a responsibility to be able to recover or restore their piece of the infrastructure.

At AT&T, our goal is to have a network where failures are prevented or identified and corrected before they affect our customers. Since 1991, we have invested more than \$300 million in our mobile network disaster recovery infrastructure and capabilities. We have also invested \$200 million in a system that proactively monitors and manages the networks of some of our largest customers.

We have more than 500 fully loaded emergency communication vehicles that we can quickly deploy to respond to any disaster anywhere in the United States. We have the basic building blocks of our network infrastructure installed in 150 technology trailers and it is ready to roll at a moment's notice.

I would like to draw on the examples of Hurricane Katrina and the 2003 blackouts to illustrate our approach to response and res-

¹ The prepared statement of Ms. Bienfait appears in the Appendix on page 139.

toration efforts and to show you how our incident command structure makes every minute count.

For Hurricane Katrina, we followed our prescribed command and control approach to a tee. AT&T began moving equipment and teams from around the country toward the Gulf States in the days before the storm made landfall. The first team restored AT&T service to its prior levels, a second team maintained and monitored AT&T's facilities so as to prevent new issues from arising, and a third team came in to help others.

AT&T worked around the clock to respond to this crisis and safeguard its network and support the efforts to respond to the disaster. AT&T was also able to direct its effort to benefit its customers, other telecommunication competitors and their customers, first responders, and evacuees, as needed. AT&T also helped to provide relief to those directly affected by the hurricane and flooding and assistance to charitable relief efforts.

Thanks to these efforts and the intense dedication of the employees involved, AT&T's network remained essentially intact. We were able to carry at least 95 percent of all calls in the Gulf Coast area that came to our network. Of the five percent of our capacity in the area that was initially lost, we restored half of that capacity within a couple of hours.

Related to the blackouts, as you know, in 2003, large portions of the Midwest, Northeast, and Ontario, Canada, experienced an electrical power blackout affecting 50 million people. Power was not restored for 4 days in some parts of the United States. Because of the reliability and redundancy that we designed and built into our network infrastructure, Internet traffic, data services, and voice calls flowed across our network without interruption.

These and other experiences have reinforced lessons that we must incorporate in future planning and are the basis of our following policy recommendations. More detailed recommendations are available in my written testimony.

Establish and practice disaster recovery processes in anticipation of emergencies. Communication resources can be brought where needed very quickly, but it is essential that those clear lines of command and control at all times are there to direct those resources effectively and to the area of greatest need. A single agency must be identified, funded, empowered to act as a national cyber incident commander for any required cyber infrastructure recovery and reconstitution efforts.

Coordinate restoration and recovery efforts. Everyone available should be participating and there needs to be coordination so the efforts are not duplicated or in conflict with one another. Logistical information, such as what roads are closed and what medical precautions are needed, must be readily available. Moreover, a recommendation we made after September 11 still has not been widely implemented. Companies such as AT&T that are crucial to the response to disasters should have special credentials designed for employees and accredited in advance in order to assess disaster areas.

Minimize the amount of regulation and data reporting requirements during a disaster and maximize the amount of coordination and cooperation between public and private sector.

Interoperability and spectrum availability. A crisis on the scale we saw in the Gulf Coast and smaller challenges, as well, demand a well-coordinated information and communications delivery system. We must resolve the spectrums needed and highlighted by the 9/11 Commission.

Consider subsidizing some of the emergency preparation by infrastructure companies. The government is likely to call on such capabilities in use or would otherwise need to duplicate resources ineffectively.

We can never anticipate every contingency in an emergency, nor can we assure a foolproof communications network all the time under all circumstances. Nonetheless, at AT&T, we have done much to ensure reliability and restorability of communication networks, and together as an industry and as a Nation, we can do more. I thank you for holding this hearing to advance this important discussion.

Chairman COBURN. Thank you, Ms. Bienfait. Mr. Aisenberg

TESTIMONY OF MICHAEL A. AISENBERG,¹ DIRECTOR OF GOVERNMENT RELATIONS, VERISIGN, INC., AND VICE CHAIR, IT SECTOR COORDINATING COUNCIL

Mr. AISENBERG. Thank you, Mr. Chairman. Thank you for the opportunity to appear before the Subcommittee today.

VeriSign's 4,600 employees operate intelligent infrastructures that enable and protect billions of interactions every day across the world's voice and data networks. I, too, have three key points I would like to make today.

First, those who make policy in the United States must understand the economic value and critical interdependencies we have developed on our information networks.

Second, we must understand and accommodate to the global nature of both our information networks and the attacks that are being continually mounted against them.

Third, largely owned and operated by the private sector, our network security and ability to withstand and recover from the continuing attacks against them depends on effective partnership between government and we, the industry stewards.

Americans must keep a clear focus on the critical economic and national security role which our information networks have come to fulfill. In less than two decades, the industrial nations have evolved an irreversible dependency and interdependency by our banking, finance, transportation, health care, education, power, manufacturing, and government service sectors on the networks managed by the companies, mostly American, which make up the ICT sector.

Each day, \$3 trillion pass over secure Federal financial networks. If these electronic transactions do not have Internet sites, such as NYSE.net, BankofAmerica.com, and Treasury.gov, available, secure, and running, the U.S. economy begins to grind to a halt at the rate of \$130 billion per hour.

As you have noted, Mr. Chairman, cyber security is indeed a responsibility which we all share and in which we all have a stake.

¹ The prepared statement of Mr. Aisenberg appears in the Appendix on page 161.

We must recognize that information networks are global, increasingly managed by interests beyond U.S. control, but at the same time subjected to threats and attacked by actors from around the world. The role of an effective government cyber security function and government-industry partnership is central to the BRT report's critical conclusion. America needs a much improved cyber security activity, not just in DHS, but across government and industry interests.

But while its conclusions are consistent with others from industry, the BRT report's suggestions about the extent and effectiveness of industry engagement with DHS are, I believe, out of touch with important progress being made in public-private collaboration in the last 18 months. There have been many, and there are increasingly significant collaborative engagements between the cyber industry and DHS, some of which were outlined by Secretary Foresman.

In 2005, commented engagement with industry began to be regularly sought by new DHS leadership. Involvement in DHS policy processes from their beginning rather than at the end began to be practiced. Examples include the national cyber security exercise Cyber Storm, concluded in February of this year, DHS's Internet Disruption Working Group, the IDWG, the government Security Operations Community, GFirst, the just-released NIPP process, and the ongoing sector-specific plans just under development.

Mr. Chairman, my sector colleagues and I have found these activities valuable and a marked departure from what we experienced prior to 2005. This steady improvement and expansion of industry involvement with DHS cyber and network security activities must continue.

But while these milestones and improvement in the relationship between cyber sector industry interests and the NCSD and NCC staff are important and significant, they are not a solution, but a beginning.

Mr. Chairman, we are at least twice as good in our cooperation as we have been, but we are not half as good as we need to be. Indeed, many of us believe that notwithstanding these improved public and private engagements, the operational posture is still fraught with risk. If a September 11-type attack were to take down the NYSE today, I doubt the Exchange could restore its network-dependent functions in the same 4 days it did in 2001, and indeed, perhaps not in 4 weeks, and the principal reason for this is DHS, or rather the bureaucratic impediments, many of which have already been discussed this morning, to the kind of action that the private sector was able to engage in in 2001 and was thwarted at during Hurricane Katrina.

We need to act without delay to ensure that our networks and critical dependent sectors are resilient enough to withstand the daily attacks being mounted against them. And as the GAO is reporting today, they must be supported by the appropriate tools from government as well as industry to assure the ability to recover with minimum collateral impact on our economy and security.

To conclude, Mr. Chairman, going forward, several steps are necessary. First, DHS's modest cyber security budget must be insu-

lated from the continuing reprogramming and budgetary cuts now underway.

Second, a cyber security leader with credibility in industry must be identified and appointed as DHS's permanent Assistant Secretary for Cyber Security and Telecommunications without further delay.

Third, critical R&D projects to improve key network security protocols must be funded and launched or relaunched.

Mr. Chairman, if we do these things, we will not guarantee that our adversaries will stop attacking our critical cyber assets, but we will improve the likelihood that we will continue to successfully withstand those attacks and retain the availability of these infrastructures on which we are now so dependent. Thank you, Mr. Chairman.

Chairman COBURN. Thank you, Mr. Aisenberg. Mr. Brondell.

TESTIMONY OF KARL BRONDELL,¹ STATE FARM INSURANCE COMPANIES, ON BEHALF OF THE BUSINESS ROUNDTABLE

Mr. BRONDELL. Thank you, Mr. Chairman. I am honored for this opportunity to testify today on Internet recovery on behalf of the Business Roundtable.

Following the attacks of September 11, Roundtable CEOs formed the Security Task Force to address ways the private sector can improve the security of its employees, facilities, communities, and our Nation. The Roundtable believes that the business community must be a partner with government in disaster preparedness and response. The Roundtable commends the Subcommittee and its members for their continued interest in improving procedures and preparedness to ensure recovery of the Internet following a major disruption. Hardening the Internet and strengthening cyber security is one of the priorities of our Security Task Force.

More than a year ago, the Roundtable began work on an initiative to assess the public and private sector plans and procedures for Internet recovery following a cyber catastrophe. We have just produced and delivered a report, "Essential Steps to Strengthen America's Cyber Terrorism Preparedness," which finds that the United States is ill-prepared for a cyber catastrophe, with significant ambiguities in public and private sector responses that would be needed to restore and recover the Internet following a disaster.

As the Subcommittee knows, the Internet and the cyber infrastructure serve as a critical backbone for the Nation's economy and its uninterrupted use is a crucial issue for our national and homeland security. But our analysis has exposed significant weaknesses that could paralyze the economy following a massive disruption.

Despite progress having been made over the past decades on technical and IT issues, there are other issues that have not received the same attention. The Roundtable's report identifies three significant gaps in our Nation's response plans to restore the Internet.

First, we found the United States lacks an early warning system to identify potential Internet attacks or determine if the disruptions are spreading rapidly across critical systems.

¹ The prepared statement of Mr. Brondell appears in the Appendix on page 167.

Second, public and private organizations that would oversee restoration and recovery of the Internet have unclear or overlapping responsibilities, resulting in too many institutions with too little interaction and coordination.

Finally, existing organizations and institutions charged with the Internet recovery have insufficient resources and support.

Collectively, these gaps mean that the United States is not sufficiently prepared for a major attack. If our Nation is hit by a cyber catastrophe that wipes out large parts of the Internet, there is no coordinated public-private plan in place to restart and restore it.

Let me make another point. Although there is no agreement among experts about the likelihood of a widescale cyber disaster, they do agree that the risks and the potential outcomes are serious enough to mandate careful planning and preparation.

In my remaining time, let me talk briefly about our recommendations for government and business to consider. We believe it is important to understand that response and recovery to a cyber disaster will be different from natural disasters when the Federal Government has the leading role. Industry must undertake principal responsibility following an incident for reconstituting the communications infrastructure and the Internet. We believe that business and government must take action, individually and collectively, to address these issues.

Let us start with the government. The Roundtable calls on the Federal Government to establish clear roles and responsibilities, to fund long-term programs, and ensure that national response plans treat major Internet disruptions as serious national problems.

Regarding the private sector, our report urges companies to designate a point person for cyber recovery, update their strategic plans, and set priorities to prepare for a widespread Internet outage and its impact on the movement of goods and services.

When it comes to protecting our Nation, neither the government nor business can do it alone. We feel the best security solutions will come from a public-private partnership that identifies and acts on ways to improve collaboration. Let me discuss a few of the collaboration recommendations.

First, since the first 24 hours often determine the overall success of recovery efforts, we must focus more attention on coordinating initial efforts to identify when an Internet attack or disruption is occurring.

Second, we recommend the creation of a federally-funded panel of experts from business, government, and academia who would assist in developing plans for restoring Internet services in the event of a massive disruption.

Finally, we believe the Department of Homeland Security, together with business, should conduct large-scale cyber emergency exercises with lessons learned integrated into programs and procedures.

Without change, our Nation will continue to use ad hoc and incomplete tools for managing our critical risk to the Internet and to our Nation's economy and its security.

Up to this point, I have outlined for the Subcommittee the basis for our observations and some of the recommendations to consider. Now I would like to spend a moment telling you about the

Roundtable's plans to find solutions to the gaps that we have identified.

First, let me say that we are confident that our member companies are able to manage most disruptions that affect Internet operations. For this reason, the Roundtable will focus its efforts on those large-scale events that no single company is positioned to manage absent widespread cross-industry and government collaboration.

As an extension of our previous work, the Roundtable will examine the processes, protocols, and practices across the private sector before, during, and after a disruptive event. We will assess which institutions respond, how early warnings are established, and how companies access information and service critical disruptions and emergency situations. We believe this will provide a foundation for meaningful improvements in our Nation's ability to protect and restore the Internet as well as clarify specific, meaningful, and actionable decisions that will lead to well-coordinated public and private response and reconstitution processes.

In conclusion, let me again thank the Chairman for the opportunity to present the Business Roundtable's report on cyber preparedness and to discuss our recommendations for improvements. Roundtable CEOs believe strongly that we need a national response to this challenge, not separate business and government responses, and that means better collaboration. I assure you, America's CEOs and our companies are committed to do their part. Thank you.

Chairman COBURN. Thank you.

One of the things I take from you all is leadership is important, and the fact that we don't have the position filled is significant. You know, that is a real problem in our Nation today and I don't know what the cause of it is. Some people say, well, the salaries aren't high enough. But for us to secure our future, we are going to have to make individual sacrifice and that means somebody out of private industry needs to come up and fulfill this role. When they are trying to recruit and nobody wants to do it because they are not willing to sacrifice a little bit of earnings for 3 or 4 years and make a commitment to make a difference to our country, we are losing the very essence of what it means to be Americans.

So it is pretty hard to hire somebody into a Federal Government agency into a position that is going to mean their salary is going to be cut in half if there is no patriotic thought that you can make a contribution to our country. Each of you have raised that. Do any one of you all want to volunteer for that position? [Laughter.]

Mr. NOONAN. I know someone that does, sir.

Chairman COBURN. Well, the man that probably is involved in that decision is sitting behind you. I hope you will communicate that with Secretary Foresman.

Mr. NOONAN. I certainly will.

Chairman COBURN. I appreciate him being here.

Just quickly, I am going to have several questions and I can't get them all through to you, so I am going to submit them in writing.

What do you think about the GAO's report? Mr. Brondell has just made a recommendation, we have got all these working groups. Here is what you all think we ought to do. We have got working

groups, yet we basically have nobody in charge. What would happen tomorrow if a major event happened? We don't have the coordination across government to the private sector to establish that. So how do we respond? How do we take your recommendation, Mr. Brondell, versus the problem? We have got working groups. We have got people that are involved in it. How do we get it off dead center and make something happen?

Mr. BRONDELL. First of all, we do applaud that the efforts are moving in the right direction. As you heard earlier this morning, it is a long road that we are going to have to pull, but as we look at a collaborative approach, we do agree and have suggested that we do need some focal point within the government that private sector can rely upon. We support the addition of the position. We hope that it gets filled quickly and goes through the administrative process to be in place.

But to your question of what we would do today if it happened, industry would continue to respond as it has in the past and overcome the hurdles based on the experience from past smaller incidents. But the lacking of collaboration, it could damage the overall economy with a long delay.

Chairman COBURN. Mr. Aisenberg.

Mr. AISENBERG. Senator, we see a steady stream of insults against the network on a daily basis. VeriSign routinely repels 1,000 or more attacks against the naming infrastructure, the DNS, every day. Major events happen with greater frequency than makes us happy, but we are successful in repelling those now, by and large. But every day, the sophistication in those attacks grows. The sources of them becomes more diverse and the risks inherent, therefore, becomes more severe.

So you are absolutely right. We need a more coordinated approach. We cannot guarantee, no one can guarantee that an attack will not at some point be successful, and I agree, the ability to reconstitute and recover from a serious attack at the moment is not as good as we need it to be, and I could not predict how severe or how long a major attack that took down the naming system or fundamental other aspects of the Internet could persist and impact the economy. Our best defense is the aggressive investment that the infrastructure stewards make in massive overhead, massive engineering, constant exercising, constant testing of the security, and vigilance, and a little bit of good luck.

Chairman COBURN. Is there an early warning system out there now?

Mr. AISENBERG. It depends on what you mean by early warning.

Ms. BIENFAIT. Not one that you would actually, as we would do with a hurricane in an emergency scenario, we see a hurricane coming and we have got a way to give an early warning—

Chairman COBURN. No, I mean is there a communication network where, whether it is NSA or whoever is experiencing it, all of the sudden, this is a major attack and time is of the essence and everybody knows it is happening in one area so they can prepare if their area is about to get hit. Is that out there now?

Ms. BIENFAIT. Not across—

Chairman COBURN. Is there an early warning system so that there is communication to all the players that something is hap-

pening. You need to know about it. Here is what we see. You might be next. Is that happening now?

Ms. BIENFAIT. We have something internal to ourselves that we can actually see the signatures and the knocking of all the hacking attacks against our network——

Chairman COBURN. That is your network?

Ms. BIENFAIT. That is my network. But we are only doing this in our own domain. We are not doing a lot across companies, across collaboration——

Chairman COBURN. Is there something that prevents you legally from being able to communicate that with the rest of the service providers?

Ms. BIENFAIT. Nothing at this point in time, other than us getting a trusted environment where we could actually do pre-planning ahead of time so that we know what that information might look like. We are doing some of that right now, trying to put best practices together, but there is not anything formal to the point that we know how to pull up a security alert and actually say, hey, the collaboration of the different units, I am going to shut down this part of my network or I am going to open up that part of my network so that this work can flow through.

Chairman COBURN. And you would all agree that is needed?

Ms. BIENFAIT. I think it is necessary.

Chairman COBURN. It is needed, and one of the reasons it is not is because there is not a position of leadership and trust which you can work through?

Ms. BIENFAIT. You really have to have a very trusted environment. It is essential——

Chairman COBURN. Otherwise you expose proprietary information.

Ms. BIENFAIT. Exactly. And we are working through that, it is just not moving fast enough.

Chairman COBURN. OK.

Mr. AISENBERG. Senator, another aspect of that is that what we call the millisecond sectors—electric power, communications, IT—frequently see insults only after they are actually mounted. Unlike intelligence gathering around physical attacks where you hear a tip from one individual and you can grow your investigative technique, very often when the attacks are mounted against the Internet or the communications or power networks, you don't see the attacks until they are already at their zero moment and are massively engaging the infrastructure.

Chairman COBURN. But, in fact, we know that is a possibility, so we can design to prevent that if we have the structure in place to communicate it, cross-communicate it without the sharing of proprietary data that would put somebody at a competitive disadvantage. I mean, that is possible. Everybody would agree with that, right?

Mr. NOONAN. Right. There is already a foundation in place, sir, but it is not broadly available cross-industry, cross-sector, cross-agency and government. There are multiple early warning activities that are operating at various levels of efficacy. These include the ISAC, the Information Sharing and Analysis Centers that are established as part of the IT, or as part of the Sector Coordinating

Councils. They are not fully operating cross-functionally today, but they are a foundation that has been being built for many years. There are issues, but we are making progress there.

I think the early warning vulnerability disclosure activity that is underway has actually moved this industry along in a number of years. If we know where our vulnerabilities are, there is a pretty good chance that is where the attacks are going to be. Whether they are malicious and disruptive or whether they are quiet and compromising, they are typically getting through our vulnerabilities.

There, I think we have made progress. However, as an industry, or both a public and private sector perspective, we don't have the equivalent of turn on CNN and get the hurricane early warning system. We simply don't have that.

Chairman COBURN. Are there any other comments from any of you all on the GAO report?

[No response.]

Chairman COBURN. I don't know if the silence is because—I won't say that. I will just let it go with that.

None of you would disagree with the fact that there could be somebody in a position that could maintain the trust of the providers and the service companies and the Internet industry and work for government and maintain the integrity that is required for us to solve these problems. Would you agree with that?

Ms. BIENFAIT. I would agree with that.

Mr. NOONAN. I would agree.

Chairman COBURN. So one of the real issues for us to move things offline is to fill the position with somebody that has the competency, character, and trust of the industry and the government and can put the impetus behind moving forward. If this hearing does anything with that, we will have accomplished something.

I want to thank each of you for being here. This is a difficult problem we face, but it is also, besides difficult, it is critical. Our country can't take many more hits. This is one that is preventable, provided we do the right thing. It is at least, if not preventable, recoverable if we do the right thing.

I would hope that we will continue to have good communications. We will have other hearings on this. We are going to move. There is going to be an Assistant Secretary, I promise you. Even if we have to raise the salary for the position, there is going to be one because it is just too important.

We will be submitting some questions to you. I would hope that you would return those to us within 2 weeks.

I thank you for your service, and the hearing is adjourned.

[Whereupon, at 11:12 a.m., the Subcommittee was adjourned.]

A P P E N D I X

STATEMENT

OF

GEORGE FORESMAN

UNDERSECRETARY FOR PREPAREDNESS
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON FEDERAL FINANCIAL
MANAGEMENT, GOVERNMENT INFORMATION, AND
INTERNATIONAL SECURITY

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

July 28, 2006

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about cyber security and the recovery and reconstitution of critical networks.

Our Nation's communications and information infrastructure will support profound improvements in the security of our homeland in the next 20 years. States, communities, and our private sector partners are already finding innovative ways to prevent terrorism and protect critical infrastructure by leveraging information technology. As I outline further below, the Federal government is similarly deploying innovative programs that significantly raise the level of preparedness in this critical area.

Our vision and philosophy for the future build upon accomplishments of the past several years – critical infrastructure businesses, home users, and government at all levels have a greater understanding of the threat posed by malicious software. The communications and information technology sectors have deployed new tools to help these constituents manage cyber risks.

However, at the core of our vision and philosophy is a strong belief that the Department of Homeland Security (DHS) must increasingly guard against more virulent attacks and cyber disruptions – whether caused by a terrorist attack or natural disaster. We must prevent cyber incidents of national significance.

In this testimony, I will outline three strategic goals to execute this vision, and examples of current and future programs that will move us forward to these objectives.

Assistant Secretary for Cyber Security and Telecommunications

As a preliminary matter, allow me to outline the steps the Department is currently taking while working with the White House to actively pursue qualified candidates for the post of Assistant Secretary for Cyber Security and Telecommunications. I am personally engaged in the process of selecting the new Assistant Secretary and, in the interim, am providing program direction pending the post being filled permanently. Because of the importance of this mission, all parties want to ensure that the individual appointed to this position possesses the right combination of skills, experience, and leadership necessary to succeed.

To supplement my own personal involvement in strategy, the Assistant Secretary for Infrastructure Protection has been serving as the Acting Assistant Secretary for Cyber Security and Telecommunications. As such, he has been actively engaged in overseeing operational programs,

program reviews, governance structure, and has participated in government/industry forums to further the advancement of this important new office as well as the strategic goals that I will outline shortly.

Regardless of when this position is filled, the mission of the Department of Homeland Security (DHS), the National Cyber Security Division (NCSD), and the National Communications System (NCS) remain clear. The absence of a permanent Assistant Secretary for Cyber Security and Telecommunication has not had an impact on NCSD's or NCS's critically important work.

Strategic Vision and Philosophy

The Assistant Secretary for Cyber Security and Telecommunications position highlights the fundamental importance the Department places on communications and information technology (IT), as well as critical linkages across the economy and our critical infrastructure sectors.

Our vision and philosophy for cyber security and recovery reflects the expanding importance of our communications and information infrastructure in all walks of life. As you know, a failure to consider and deploy effective strategies could adversely affect homeland and national security, public health and welfare, and our economic security. Policies that advance a safe and secure communications infrastructure promote public trust and confidence, project stability to those who wish us harm, and foster valuable relationships between the public and private sectors.

We fully recognize the challenges inherent in our preparedness responsibilities. We are faced with difficult choices and options. We must think about risks to the communications and information infrastructure in new and creative ways. We must prioritize resources, and make hard decisions where resources are limited.

We must also continue to partner strategically with the communications and information technology sectors as well as other experts outside of the Federal government. As we focus on the potential for catastrophic cyber disasters, our partnerships are becoming more diverse and sophisticated, reflecting the different technology, business, and policy decisions that must be made. These partnerships also entail strengthening cooperation across the government and, at a minimum, finding ways to cultivate support outside of the Department where expertise clearly exists. Whether public or private, the partnerships must deliver real and measurable value in light of the catastrophic damages that can occur in the absence of smart collaboration.

Finally, we must reinforce a culture of preparedness and increasingly shift from a reactive to a proactive stance. In sum, we must prepare by promoting effective security strategies that evolve as the threat evolves.

Three Strategic Goals

In responding to these challenges, the Preparedness Directorate is executing three strategic priorities. (1) We are preparing for cyber incident of national significance; (2) we are working to forge more effective partnerships; and (3) we are working to foster a culture of preparedness to prevent cyber incidents and mitigate damage when disruptions occur.

➤ First, we must prepare for a large scale cyber disaster.

Our primary strategic goal is to prepare for high-consequence incidents. These would include, for example, a widespread disruption involving the Internet or critical communications infrastructure, whether from an attack or natural disaster.

Now, as the Department matures we are preparing for large scale cyber disasters. Our strategic intentions are ambitious and will require resolution of multiple impediments, such as:

- Identifying incidents and providing early warning;
- Deploying Federal assets and services more efficiently to mitigate damages where disruptions occur;
- Responding to the speed of attacks and disruptions, which will require new technologies and skill sets in our workforce; and
- Maximizing the use of tools that promote and integrate privacy protections as well as real-time security needs.

The Preparedness Directorate has several important programs already underway to prepare for a cyber incident of national significance. The Office of Cyber Security and Telecommunications has established an Internet Disruption Working Group (IDWG) to address the resiliency and recovery of Internet functions in the event of a major cyber incident. The IDWG is not examining all risks, but is focusing on and identifying measures that government and its stakeholders can take to protect against nationally significant Internet disruptions.

These proposed measures may yield heightened expectations, roles, and responsibilities for the United States Computer Emergency Readiness Team (US-CERT).

➤ **Second, we must continue to forge more effective partnership arrangements.**

Our second strategic goal is to improve the Department's partnership programs and practices. Homeland Security Presidential Directive 7, the Administration's policy on critical infrastructure protection, explicitly recognizes the importance of partnerships, which are essential for many sound reasons. In the cyber security arena, the Department is working to nurture existing partnerships and establish new relationships with three key stakeholder communities: (1) the private sector; (2) Federal departments and agencies and State, local, and tribal governments; and (3) academia.

Private Sector Partnerships. Industry owns, operates, and controls the bulk of the communications and information infrastructure, so collaborating with industry to prepare for and respond to catastrophic cyber disasters is a strategic priority.

In "The Federal Response to Hurricane Katrina: Lessons Learned," the White House pinpointed specific problems experienced by infrastructure owners in restoring communications services. The report additionally described interdependencies between the critical infrastructure sectors, such as energy and transportation, that impact restoration of communications services. Our vision for the future, and emphasis on close collaboration with the private sector, follows directly from these lessons learned.

In our partnerships, the government must deliver real value to our private sector partners, who are clearly committed to a collaborative approach. Smart, effective partnerships demand that we:

- Understand how the private sector will prepare for and respond to cyber disasters – and where the government can complement industry practices;
- Leverage state of the art technologies to improve preparedness and response and sustain privacy protections;
- Promote pools of knowledge and subject matter expertise for reconstituting communications and information infrastructure; and
- Ensure close coordination of Preparedness Directorate functions, such as those provided by NCSD and NCS,

Government Partnerships. The Department is similarly committed to enhancing partnership arrangements across the Federal government and

with State, local, and tribal governments. We will continue to explore innovative ways to leverage skill sets outside of the Department as part of our strategy for cyber-preparedness and response. We currently partner with Multi-State Information Sharing and Analysis Center (MS-ISAC), as well as a key operational information technology and communications officials in the states, and we are strengthening those partnerships for recovery and reconstitution efforts.

Partnerships with Academia. The Department is serious about partnering aggressively with experts in academia. To date, the Department has included academia in partnership discussions; however, in order to lay a foundation for more effective cyber response capability, we must seek guidance from academia on a range of more complex problems. As an example, we expect to learn more from academia on such matters as challenges with insurance and risk transfer for the critical infrastructure sectors as well as business case arguments for catastrophic preparedness. These areas promote public and private sector collaboration.

Third, we must create a culture of preparedness – both to prevent a cyber disaster and to mitigate damages if widespread disruptions occur.

Our third and final strategic goal seeks to influence how we prepare for security challenges in the coming decade. As with our other strategic priorities, this goal demands a focused and disciplined approach in several areas. At a minimum, we are structuring programs to:

- **Clearly outline preparedness organizations, relationships, and expectations:** One of the Preparedness Directorate's strategic priorities is to clearly set forth all aspects of "doctrine" in accordance with legislative and Presidential direction. To create a long-term culture of preparedness, we are developing clear organizational doctrine, which memorializes strategic policies, clarifies roles and responsibilities, and defines measures of accountability.
- **Promote a shared way of life that measurably improves preparedness for a catastrophic cyber disaster:** Finally, we are focusing our energies on cyber-preparedness. Our programs in the coming years will seek to inculcate to change behavior as we continue to leverage our government partners to help continue efforts in these other areas. Awareness and education in the past decade have focused on large segments of the population, including home users and students in K-12. We hope to develop additional awareness programs that look more carefully at catastrophic cyber risk and continue to leverage our government partners to help advance our efforts in these other areas.

Organizational Framework

The three strategic goals outlined above will require clear organizational directions and programs.

HSPD-7 directs the Department to establish an organization dedicated to cyber security. The Preparedness Directorate's National Cyber Security Division (NCS) has been that organization since it was created in June 2003. Since its inception, the NCS has taken on the broad mandate of HSPD-7 and those provided in the President's National Strategy to Secure Cyberspace, in its mission to work collaboratively with private, public and international entities to secure cyberspace and America's cyber assets.

The NCS is just one of the valuable preparedness resources within the Department. As part of the Preparedness Directorate, the NCS works closely with the Office of the Manager of the National Communications System (NCS), which addresses national security and emergency preparedness (NS/EP) telecommunications. These two entities comprise what is now the Office of Cyber Security and Telecommunications. The Office of Cyber Security and Telecommunications works closely with the Office of Infrastructure Protection to ensure that the ever increasing interconnected nature of physical and cyber security is integrated throughout our overall preparedness efforts.

The National Communications System consists of 23 Federal departments and agencies with assets, resources, requirements and/or regulatory authority regarding national security and emergency preparedness (NS/EP) communications. Established pursuant to Executive Order 12472, the community is administered by DHS as Executive Agent and Manager and it supports the Executive Office of the President (the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget) in the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.

Executive Order 12472 also mandates inclusion of an industry component, the National Coordinating Center (NCC) for Telecommunications, or NCC Watch, a joint industry/Government body operating a 24 hour, 7-day a week watch center to coordinate NS/EP communications activities. The NCC Watch has a unique relationship with members of the private telecommunications sector in the

Communications Information Sharing and Analysis Center (ISAC). The Communications ISAC provides an opportunity for private sector industry to partner with government to exchange information and coordinate restoration of communications assets and services during emergencies. In this role, the NCC Watch communicates daily and shares a web-portal with NCSD (US-CERT) on cyber related issues.

To meet its mission, the NCSD is focused on leading a cyber risk management program, and building and enhancing the National Cyberspace Response System. To address these priorities, the NCSD is engaged in a public-private partnership which is incorporated into all of NCSD's programs. This is especially critical since the vast majority of our national assets and critical infrastructure are owned and operated by the private sector.

National Cyber Risk Management Program

The National Cyber Risk Management Program reflects the Department's overall strategic approach that is focused on risk management, as outlined in the National Infrastructure Protection Plan (NIPP). The NIPP incorporates the Department's overall risk management framework to assess and reduce our cyber risk, and improve our planning for response, recovery, and reconstitution of our critical networks.

- The Department released the NIPP on June 30 of this year after consultation with industry. The NIPP formalizes the collaboration between government and industry through the Sector Partnership Model with Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC) working together to address risk by analyzing consequences, vulnerabilities, and threats.
- The NIPP provides a unifying structure for protection of the Nation's 17 critical infrastructure and key resources (CI/KR) sectors designated in HSPD-7, including the Information Technology Sector and the Internet. The NIPP calls upon each sector to develop a Sector Specific Plan based on the risk management framework. DHS is the Sector Specific Agency (SSA) responsible for both the Information Technology Sector and the Communications Sector, and assists other sectors with the cyber elements of their infrastructure. The NCSD works closely with the IT Sector Coordinating Council, which was formally launched in January of this year. The IT-SCC and IT-GCC are working together on the IT Sector Specific Plan, which will be completed at the end of the year.

- In order to accomplish the risk management objectives of the NIPP, we have been working closely with the private sector to build the framework required. To facilitate the development of this partnership, the Department has established the Critical Infrastructure Partnership Advisory Council (CIPAC). The CIPAC comprises representatives from each of the critical infrastructure and key resources (CI/KR), sectors, SCCs, and GCCs, and provides a mechanism for the information exchange and collaboration between industry and government that is so crucial to understanding the risk we face. The Council also prioritizes the protective measures that need to be taken to reduce that risk.

As we develop the IT Sector Specific Plan and deepen our collective understanding of the cyber risks in other sectors, we are building the foundation for the development of a national cyber risk assessment. Working with our government and private sector partners, we are taking steps, such as developing attack scenarios and conducting red cell workshops and exercises, to identify what we are most concerned about in cyberspace, and then using that information to build our response and mitigation plans. As part of our risk management efforts, we have three priority mitigation programs.

First, as discussed above, the Office of Cyber Security and Telecommunications has established an IDWG to address the resiliency and recovery of Internet functions in the event of a major cyber incident. The IDWG is working with government, private sector, academic and international security experts to examine risks, improve preparedness and situational awareness, and identify measures that we can take to protect against nationally significant Internet disruptions. The IDWG conducted a tabletop exercise in June to examine the kinds of scenarios that would have significant impact on the Internet, understand when information exchange between the public and private sector is mutually beneficial, and to determine what roles and responsibilities industry and government should assume in responding to and recovering from such disruptions.

Second, the NCSD is collaborating with the national laboratories for its Control Systems Security Program to bring together government, industry, and academia to address the threats and vulnerabilities of the process control systems that remotely operate and control access to many of our critical infrastructure assets and systems. To support the Program, NCSD has established a US-CERT Control Systems Security Center, which is an assessment and incident response facility located at Idaho National Laboratory. The department also partners with the

industry sectors that utilize process control systems in their operations through the Process Control Systems Forum, or “PCSF”. The PCSF met recently in San Diego and furthered its work to accelerate the security of control systems, provide a venue for sharing perspectives on cross-sector security issues, and facilitate solution-driven collaborative workshops.

Through the Process Control Systems Forum (PCSF), the Department also partners with the industry sectors that utilize process control systems in their operations. The PCSF met recently in San Diego and furthered its work to accelerate the security of control systems, provide a venue for sharing perspectives on cross-sector security issues, and facilitate solution-driven collaborative workshops.

The third risk mitigation effort is NCSD’s Software Assurance Program that seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities. In collaboration with industry, academia, and government partners, the Department’s approach to addressing software assurance identifies the following as keys to success:

- People – education and training for developers and users
- Processes – practical guidelines and best practices for the development of secure software
- Technology – tools for evaluating software vulnerabilities and quality
- Acquisition – specifications and guidelines for acquisition and outsourcing

To further its efforts, the Software Assurance Program holds semi-annual Software Assurance Forums with other Federal agencies, industry, academia, and international entities to facilitate ongoing collaboration and progress. As part of the program, NCSD has launched “Build Security In” to raise awareness and foster collaborative efforts.

The Office of Management and Budget (OMB) has recently designated NCSD as the Managing Agency for the Information Systems Security Line of Business. As part of NCSD’s work with the Federal government, NCSD is currently working to establish a Program Management Office for this government-wide initiative which has an overarching goal of improving the effectiveness and consistency of systems security across the Federal enterprise. This effort will reduce costs through consolidation and standardization of resources. DHS will be working closely with partner agencies in overseeing the implementation of information systems security products and services.

In order to reduce our collective cyber risk we need to raise awareness of cyber security vulnerabilities and understand what we must do as individuals to create a collective, shared secure cyber infrastructure.

NCSD's awareness program leverages partnerships with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the National Cyber Security Alliance (NCSA), as well as our own National Cyber Alert System to reach state and local governments, small businesses, home users, and K-12 and higher education audiences. October is National Cyber Security Awareness Month. In October 2005, together with our state government and industry partners, we reached millions of Americans with a public service announcement, a satellite media tour on how to avoid identity theft in cyberspace, a national cyber awareness webcast for fourth and fifth graders, and many other activities. We look forward to making this year's campaign even more successful.

Cyber space is borderless, and as such, managing cyber risk needs to take into account international activities. NCSD has an international affairs program that seeks to address cyber security globally through cooperation and collaborative action toward building and leveraging the relationships needed to prevent, protect against, respond to and recover from cyber incidents and reduce overall cyber risk.

National Cyberspace Security Response System

There are three elements to the National Cyberspace Security Response System: the U.S. Computer Emergency Readiness Team Operations, or "US-CERT Ops"; the National Cyber Response Coordination Group, or "NCRCG"; and our regional preparedness and recovery efforts.

The first key element, US-CERT, was established in 2003 as a partnership between the Department and the public and private sectors to protect the nation's critical infrastructure and coordinate defense against and responses to cyber attacks. The US-CERT public website, <http://www.us-cert.gov>, the secure portal for stakeholders, and the National Cyber Security Alert System, provide timely, actionable information to technical and non-technical users. We encourage each of you to sign up for the US-CERT cyber alerts by going to <http://www.us-cert.gov>.

NCSD/US-CERT has an Operations component, which manages many aspects of the Cyberspace Security Response System, including situational awareness, incident handling and response, malicious code analysis, and strategic operations. Under Federal Information Security Management Act guidelines, OMB requires all Federal civilian agencies to notify US-CERT of any data breaches, unauthorized access, or

suspicious activity, including the loss of personally identifiable information within one hour of discovery.

US-CERT maintains a 24x7 secure Watch center; acts as a trusted third party to assist in the responsible disclosure of vulnerabilities; develops and participates in regional, national, and international level exercises; supports forensic investigations with recursive analysis on artifacts; provides malware (software that is designed to infiltrate or damage a computer system, without the owner knowing) analytic and recovery support for government agencies; coordinates Federal programs of computer emergency response teams and Chief Information Security Officer peer groups for sharing cyber incident information, best practices, and other cyber security information; and, collaborates with national and international computer security incident response teams both in the US and abroad. US-CERT's efforts in these and additional areas build our cyber situational awareness capabilities that allow us to prepare for and defend against cyber attacks, while also enhancing our ability to respond to the attacks.

US-CERT has established the Government Forum of Incident First Response Teams (GFIRST), a community of Federal agency incident response teams, which comprises the government's critical group of cyber first responders. GFIRST meets regularly, and we have hosted two GFIRST conferences to enhance information sharing and collaborative efforts to secure government cyberspace. US-CERT provides an Internet Health Service tool to GFIRST members through the US-CERT secure portal. IHS is a web-based application that provides members with access to several commercially available Internet and security products for use in building their situational awareness capabilities through the monitoring of their respective networks and the overall health of the Internet. In addition, as part of our Situational Awareness Program, US-CERT also leverages information technology for the automated sharing of critical information across the Federal government and analysis of traffic patterns and behavior.

US-CERT has developed a set of informational resources that it provides to our public and private sector stakeholders, including alerts, vulnerability notices, current activity reports, Federal Information Notices provided to the GFIRST community and Critical Infrastructure Information Notices provided to the private sector Information Sharing and Analysis Centers. In addition, US-CERT runs the National Cyber Alert System and the public website reference above, which provide cyber security tips, guidance, and other resource materials to technical and non-technical audiences.

The second key element of the National Cyberspace Security Response System is the National Cyber Response Coordination Group, or “NCRCG”. NCSD co-chairs the NCRCG with its counterparts in the Department of Justice and the Department of Defense. The NCRCG includes 13 agencies with responsibility for and capabilities in cyber security matters and works to coordinate national response activities to incidents of national significance. The NCRCG meets monthly to prepare for cyber issues through tabletop exercises and working groups.

In addition to the IDWG’s efforts and US-CERT Operations incident handling and analysis functions, the NRP’s Emergency Support Function 2 (ESF-2) for Communications, led by NCS, is a critical component of advanced planning and ensuring coordinated recovery efforts. When ESF- 2 is activated, the Manager of the NCS ensures appropriate NS/EP communications support to operations conducted under the NRP. As part of ESF-2, NCSD works closely with NCS on preparing for recovery and reconstitution of critical communications networks and services. In preparation for this year’s hurricane season, we have held ESF-2 training and exercise sessions with participation by many Federal agencies and organizations. We have created and published an ESF-2 Operational Plan and a Standard Operating Plan for ESF- 2 supporting agencies to enhance understanding across the spectrum of public and private sector entities that participate in recovery and reconstitution efforts. We have hired two Regional Communications Coordinators for Federal Regions IV and VI communications pre planning with state emergency planners. The NCS has also created more analytical tools for predictive and post-impact analysis.

One of the critical parts of ESF-2 is a management function to coordinate and facilitate the handling of private sector donations for recovery and reconstitution efforts in the immediate aftermath of a disaster such as Hurricane Katrina. We are working with our private sector stakeholders and state and local government partners to establish a set of requirements for such donations in order to match those needs with the products and services available.

The third key element of the National Cyberspace Security Response System is our regional preparedness and recovery efforts. Our regional efforts have greatly improved DHS’s ability to incorporate the work of our government and private sector stakeholders at both the state and local levels. The Pacific Northwest Economic Region and the Gulf Coast Region are increasingly coordinating their efforts as a result of exercises held in the respective regions, and we are working with them to continue their preparedness planning for both cyber security events, and manmade or natural disasters that have a cyber impact. In addition, we are working with our industry stakeholders in the IT-SCC and IT

Information Sharing and Analysis Center) to develop plans for industry assistance in the event of an incident that requires surge support to recover and reconstitute critical IT systems. These efforts depend greatly on our partnerships with the full spectrum of affected industries, state and local government stakeholders, and the emergency response community.

Recent Success Stories

I would like to take this opportunity to highlight two recent success stories in our comprehensive cyber security efforts. First, we conducted the first National Cyber Exercise organized and sponsored by the Federal government. Conducted in February 2006, "Cyber Storm" was the largest multinational, cross-sector cyber exercise to date and assessed policies and procedures associated with a cyber-related incident of national significance, as outlined in the National Response Plan's Cyber Annex. The exercise tested, for the first time, the full range of cyber-related response policy, procedures, and communications methods required in a real world crisis.

Cyber Storm exercised the responses of over 100 public and private agencies, associations, and corporations in over 60 locations and five countries. It achieved collaboration in crisis response at operational, policy, and public affairs levels, including participation of more than 30 private sector corporations and associations in the planning, executing, and after action analysis of a federally funded and congressionally mandated emergency response exercise. As mentioned earlier, Cyber Storm exercised the NCRCG as the principal Federal mechanism for coordinating the national response to a cyber incident of national significance. Cyber Storm demonstrated the close cooperation and information sharing needs across Federal agencies, across boundaries, and between the public and private sectors.

First, the exercise reinforced the importance of defining roles and responsibilities, processes and procedures and having strong communications and coordination among the cyber community. In addition, it highlighted the importance of coordinating and integrating incident communications and public affairs outreach. Unlike a physical, self-announcing incident, a set of cyber attacks such as those imagined in the Cyber Storm scenario are not immediately apparent, either in occurrence or attribution. The correlation of multiple incidents proved challenging for our players, and only further demonstrated the importance of public-private relationships and the need to provide on-going training activities, discussions, and exercises to further build those relationships to strengthen our collective response to a cyber incident.

We are currently making improvements to our policies and procedures to address key findings, and have begun the planning process for Cyber Storm 2, which is slated for 2008.

A second accomplishment falls in the international arena. At the end of June, we successfully hosted here in Washington the second multilateral conference on the development of an International Watch and Warning Network, or "IWWN", among 15 countries in the Americas, Europe, and Asia Pacific. The country participants included representatives from their government critical information infrastructure protection organizations, their computer security incident response teams, and their law enforcement agencies with responsibility for cyber crime. The IWWN was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities. The June conference established a clear path forward for the IWWN community to enhance global cyber situational awareness and incident response capabilities and marked the launch of a secure Internet portal to facilitate ongoing international information sharing as well as coordination during cyber incidents.

The Road Ahead

As we further develop our programs and leverage our recent successes, there are some efforts we need to undertake in the near term with our industry and agency partners to better prepare ourselves to respond to, and recover from, cyber incidents. These efforts include, but are not limited to:

- Further integration of the cyber security and telecommunications efforts in the Department and with industry to reflect increasing convergence in the sectors;
- Clearer articulation of roles and responsibilities in the public-private partnership for information sharing and incident response through coordinated concept of operations and standard operating procedures;
- Development of the IT Sector Specific Plan in the NIPP risk management framework;
- Development of a national cyber risk assessment based upon the cross sector cyber component of the NIPP risk management framework;
- Share aggregated situational awareness across the civilian agencies, the military, the international community, and the private sector; and
- Further collaboration between US-CERT Operations and the Department of Defense's Joint Task Force-Global Network

Operations to leverage our respective expertise and capabilities toward common cyber security objectives.

These efforts are being undertaken in the Cyber Storm After Action planning, the NIPP process, our international engagements, and our collaboration with industry on all of our programs. These action plans have defined benchmarks and milestones to drive and track our progress in each of these areas.

Conclusion

The National Cyber Security Division has established its mission and priority objectives, developed a strategic plan, and undertaken significant steps to implement its strategic plan across the programs outlined here. In this ever-evolving environment, we know that the target will shift to accommodate new threats, new vulnerabilities, and new technologies. We need to be flexible enough to adjust our efforts to meet these new challenges.

Our progress to date is tangible: we have a construct for public-private partnership; we have a track record of success in our cyber operations; we have established relationships at various levels to manage cyber incidents; we have built international communities of interest to address a global problem; and we have tested ourselves at a critical development stage and will continue to examine our internal policies, procedures, and communications paths in future exercises. We are building on each of these achievements to take further steps to increase our cyber preparedness and improve our response and recovery capabilities.

I would like to thank the Subcommittee for its time today and I appreciate this opportunity to bring further transparency to these important cyber security priorities.

Cyber Security: Recovery and Reconstitution of Critical Networks

**PREPARED STATEMENT OF RICHARD C. SCHAEFFER, JR.,
DIRECTOR OF INFORMATION ASSURANCE, NATIONAL SECURITY AGENCY**

July 28, 2006

Good afternoon Mr. Chairman and distinguished members of the Subcommittee. My name is Richard C. Schaeffer, Jr., and I am the National Security Agency's (NSA) Information Assurance Director. I appreciate the opportunity to be here today to talk briefly about the NSA's information assurance mission and its relationship to the work of the Department of Homeland Security and others concerned with helping operators of crucial information systems prepare for and recover from hostile acts or other disruptive events.

I would also like to thank the Chairman and the other members of the Subcommittee for their continued interest in, and attention to, this issue. Each day, ever more data and functions that are vital to the nation are consigned to digital systems and complex, inter-dependent networks. There are no "silver bullets" when it comes to cyber security, but over time, increased awareness of cyber security issues, new standards, better education, expanded information sharing, more uniform practices, and improved technology can and do make a meaningful difference.

The NSA information assurance mission focuses on protecting what National Security Directive 42 defines as "national security information systems" that handle classified information or are otherwise critical to military or intelligence activities. Historically, much of our work has been sponsored by and tailored for the Department of Defense. Today, national security systems often rely on commercial products or infrastructure, or interconnect with systems that do. This creates new and significant common ground between defense and broader U.S. Government and homeland security needs. More and more, we find that protecting national security systems demands teaming with public and private institutions to raise the information assurance level of products and services more broadly. If done correctly, this is a win-win situation that benefits the whole spectrum of information technology (IT) users, from warfighters and policymakers, to federal, state, and local governments, to the operators of critical infrastructure and major arteries of commerce.

This convergence of interests has been underway for some time and we can already point to several examples of the kind of fruitful collaboration it inspires. For instance, the NSA and the National Institute of Standards and Technology (NIST) have been working together for several years to characterize cyber vulnerabilities, threats, and countermeasures, to provide practical cryptographic and cyber security guidance to both IT suppliers and consumers. Among other things, we've compiled and published security checklists that harden computers against a variety of threats; we've shaped and promoted standards that enable information about computer vulnerabilities to be more

easily cataloged and exchanged and, ultimately, the vulnerabilities themselves to be automatically patched; and we've begun studying how to extend our joint vulnerability management efforts to directly support compliance programs such as those associated with the Federal Information Security Management Act. All of this is unclassified and advances cyber security in general, from national security and other government networks to critical infrastructure and other commercial or private systems.

The NSA partners similarly with the Department of Homeland Security (DHS). In 2004 DHS joined the NSA in sponsoring the National Centers of Academic Excellence Program to foster training and education programs to support the nation's cyber security needs and increase the efficiency of other Federal cyber security programs. As of June of this year, 75 such centers have been established across 32 states and the District of Columbia, including Oklahoma, Alaska, Ohio, New Mexico, Virginia, Michigan, Minnesota and New Jersey. The NSA supplies trained personnel and other technical support to the U.S. Computer Emergency Readiness Team and we routinely alert one another to possible or emerging hostile cyber acts. In fact, DHS has just named an integree to work in the NSA/Central Security Service (CSS) Threat Operations Center, which has as one of its missions to monitor the operations of the global network in real time to identify network-based threats to DoD and Intelligence Community networks.

NSA and DHS cooperate on investigations and forensic analysis of cyber incidents and malicious software, and together we look for and mitigate the vulnerabilities in various technologies that would render them susceptible to similar attacks. We each bring to these efforts complementary experience, insight, and expertise based on the different problem sets and user communities on which we concentrate, and we each then carry back to those communities the dividends of our combined wisdom and resources.

With regard to post-incident response, the NSA supplies technical personnel, advice, and equipment to support an efficient response and recovery to disasters. The NSA has worked with the DHS Infrastructure Protection Division to plan for the interoperable communications systems needed to support response and recovery. The NSA maintains a stock of secure communications equipment to replace or augment deployed systems in the wake of emergencies or other urgent and unforeseen needs. Following Hurricane Katrina, the NSA supplied encryption devices, secure satellite telephones, and cryptographic keying material to many DoD and civil entities involved in rescue and recovery. We also helped the National Aeronautics and Space Administration (NASA) reestablish secure connectivity between the Stennis Space Center near Bay St. Louis, Mississippi, NASA headquarters in Washington, and NASA's Marshall Space Flight Center in Huntsville, Alabama. When it comes to reconstructing networks beyond just communications systems, bringing in replacement technology may be the easy part. The real challenge is knowing *what* to reconstruct. That means maintaining an up-to-date understanding of what set of data, functions, and connections – available to what set of users – qualify as critical. It also requires regular mapping and analysis to track the shifting physical and logical make-up of these nets.

Looking forward, NSA and DHS interests will continue to merge and the opportunities – and need – for shared work and mutual support will continue to grow. As once unique environments such as national security systems, computerized industrial controls (i.e., supervisory control and data acquisition, or SCADA systems), emergency services

communications, and specialized financial and logistical networks come to rely on the same commodity hardware, software, commercial infrastructure and services, we find ourselves concerned with many of the same vulnerabilities, threats, and countermeasures. We both have a stake in expanding the market for secure information technology and in steadily raising the bar when it comes to defining what's secure and what isn't. We both have a responsibility to help IT suppliers improve their products and to help IT buyers and operators make more informed choices about what to buy and how to assemble, configure, run, monitor, and defend their systems. Since none of this is possible without security-savvy IT professionals, information assurance education and training remains a joint imperative.

Finally, beyond technical convergence, in the post 9/11 world the NSA and DHS are also bound together by the need to provide for communications across once unbridgeable chasms of classification and practice, from the President all the way to first responders and the owners and operators of critical infrastructure. As a starting point, the NSA and NIST have established a suite of unclassified cryptographic standards that can be implemented in commercial-off-the-shelf offerings as well as specialized high-end government equipment. This sets the stage for interoperable encryption and message authentication and is an important step -- although just one step -- in the broader effort to ensure that the nation can recognize and respond to impending emergencies or their aftermath.

Once again, thank you Mr. Chairman for giving me the opportunity to appear before you today, and I will be happy to answer any questions you may have.

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, AND INTERNATIONAL SECURITY
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

July 28, 2006

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about cyber security: recovery and reconstitution of critical networks.

The President has directed Federal agencies to work with State and local governments as well as the private sector to enhance the protection of our Nation's critical infrastructure. The Department of Homeland Security (DHS) is coordinating this effort.

The Office of Management and Budget (OMB) oversees the implementation of government-wide policies, standards, and guidelines for the Federal government's information technology security programs. My testimony today will focus on OMB activities to improve the security and resilience of the Federal government's critical cyber assets.

Maintaining Telecommunication Services During a Crisis or Emergency

Last year, the Director of OMB issued a regulation (M-05-16 dated June 30, 2005) on maintaining telecommunication services during a crisis or emergency. This regulation was issued in response to Section 414 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act. The regulation required each agency to review its telecommunication capabilities in the context of planning for contingencies and continuity of operations situations.

OMB also asked each agency to confirm they were complying with directives issued by the National Communications System (NCS) and guidance issued by the Federal Emergency Management Agency (FEMA). As background, NCS was established by Executive Order 12472 in 1984 and has a unique status and set of responsibilities regarding national security/emergency preparedness (NS/EP) telecommunications within the federal government. NCS directives establish policies and procedures for NS/EP telecommunications, and FEMA

provides guidance to Federal Executive branch departments and agencies for use in developing contingency plans and programs for continuity of operations.

In August 2005, all large agencies submitted reports on the status of their telecommunication services. In addition, forty small and independent agencies provided the requested information. OMB and NCS worked together to review the responses. Our analysis revealed the need for additional guidance to the agencies regarding the use of redundant and physically separate telecommunications service entry points into buildings and the use of physically diverse local network facilities.

In October 2005, the NCS hosted a Route Diversity Forum outlining route diversity theory and highlighting the procedures for agency self-assessment and NCS suggested ways to ensure adequate route diversity. Over seventy Federal agency representatives attended the forum. NCS has recently developed a Route Diversity Methodology enabling agencies to self-assess their facilities to determine their level of route diversity. Information regarding this methodology is available on the NCS website.

Procurement of Telecommunication Services

When an agency initiates new telecommunications procurements, the agency must determine the appropriate level of availability, performance and restoration that is required, in accordance with the agency's continuity of operations plans.

The General Service Administration's Networkx program will serve as the primary replacement for the expiring FTS2001 telecommunications contracts. The Networkx procurements will specify telecommunications infrastructure security requirements to protect contractor network services, infrastructures, and information processing resources against cyber and physical threats, attacks, or system failures. Networkx contractors must comply with security law and policy such as OMB Circular A-130, the Federal Information Security Management Act and the National Institute of Standards and Technology Federal Information Processing Standards.

In developing Networkx, GSA has defined a full spectrum of Security Services to meet individual agency needs. These include Managed Tiered Security Service with different network security levels, Managed Firewall Service, Intrusion Detection and Prevention Service, Managed E-Authentication Service, Vulnerability Scanning Service, Anti-Virus Management Service, Incident Response Service, and Secured Managed E-mail Service.

With regard to recovery and reconstitution of critical networks, the Networkx program specifies telecommunications requirements for compliance with NS/EP directives, as established by the NCS in accordance with Executive Order 12472. This will ensure that Networkx telecommunications capabilities are continuously ready to meet the needs of Federal agencies during national emergencies. Additionally, Networkx will fully interoperate with the NCS's Government Emergency Telecommunications System and Wireless Priority System.

Identification and Protection of Critical Cyber Infrastructure

On December 17, 2003, the President signed Homeland Security Presidential Directive (HSPD) -7, "Critical Infrastructure Identification, Prioritization and Protection." This directive established the national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

HSPD-7 required the heads of all Federal agencies to develop and submit to the Director of OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they owned or operated. The plans were due July 31, 2004. All agencies with HSPD-7 responsibilities submitted the protection plans.

In OMB's reporting guidance, we asked agencies to address critical infrastructure identification, prioritization, protection, and contingency planning to include the recovery and reconstitution of essential capabilities. Twenty four agencies confirmed they owned or operated nationally critical systems and assets. These are assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, or public health or safety.

OMB worked with DHS' National Cyber Security Division to develop scoring criteria and evaluate the protection plans. We provided each agency with a written response explaining our approval or disapproval of the agency's cyber security plan and highlighting areas where improvement was needed.

The evaluations conducted in 2005 have been used to inform DHS' development of the National Infrastructure Protection Plan (NIPP). The NIPP will provide for a more detailed analysis of critical infrastructure inside the federal government.

In May 2005, OMB added continuity of operations planning criteria to the President's Management Agenda scorecard. All agencies wishing to maintain green status on the E-Government scorecard are required to test their contingency plans on an annual basis. OMB tracks statistics related to contingency plan testing through quarterly performance updates provided by the agencies in fulfillment of Federal Information Security Management Act (FISMA) policies.

Improving the Security of Federal Information Systems

Each year, as required by FISMA, agency Chief Information Officers and program officials conduct IT security reviews of the systems that support their programs. Additionally, agency Inspectors General are asked to perform annual independent evaluations of the agency's IT security program and a subset of agency systems. The results of these reviews are reported annually to OMB. As part of their evaluations, agencies are asked to categorize their information systems, including contractor systems into high, moderate, or low impact and

document the security controls implemented for each. OMB has stated as a rebuttable presumption all cyber critical infrastructure and key resources identified in an agency's HSPD-7 plans are high impact as are all systems identified as necessary to support agency continuity of operations. Systems necessary for continuity of operations purposes include for example, telecommunication systems identified in agency reviews under OMB's regulation on maintaining telecommunications service during a crisis.

OMB has found agency senior managers are paying greater attention to IT security. Chief Information Officers maintain plans of action and milestones (POA&Ms) to ensure program and system level IT security weaknesses are tracked and corrected. The agencies include in their plans the name of the person responsible for correcting the weakness, the resources required and the target completion date. The plans are updated by the agencies on a quarterly basis and agencies report their status and progress to OMB. These updates help to inform the quarterly assessment of the President's Management Agenda scorecard.

Incident Response

The National Cyber Response Coordination Group (NCRCG) is the principal federal interagency mechanism to coordinate preparation for and response to cyber incidents of national significance. The group is co-chaired by DHS, the Department of Justice and the Department of Defense. OMB is a member of the group along with other agencies having a statutory role in cyber security, cybercrime, or protection of critical infrastructure. Member-agencies meet on a monthly basis to identify issues and concerns.

During a cyber incident, the member agencies would integrate their capabilities in order to assess the scope and severity of the incident, govern response and remediation efforts, and guide senior policymakers. The NCRCG would use their established relationships with the private sector and state and local governments to help manage a cyber crisis and develop recovery strategies.

In February 2006, DHS sponsored the national level cyber exercise "Cyber Storm." During this exercise, NCRCG member agencies tested their concept of operations as well as communications with critical infrastructures. Additionally, in June 2006, DHS staged the fourth Top Officials Command Post Exercise (TopOff) to test the government's response to terrorist events. The exercise involved over 4,000 representatives from federal, state and local governments along with private sector participants.

Conclusion

In conclusion, each agency is responsible for ensuring the continued availability of its mission essential and national security/emergency preparedness telecommunications services. Strategic improvements in security and continuity of operations planning can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. The Administration is committed to a federal government with secure and resilient information systems. We will continue to work with agencies, Congress and the GAO to ensure appropriate risk-based and cost-effective IT security programs, policies and procedures are put in place to protect the Federal government's critical cyber infrastructure.

**United States- Computer Emergency
Readiness Team
US-CERT**

**Concept of Operations for Federal Cyber
Security Incident Handling**



April 2005
Version 3.2

FOR OFFICIAL USE ONLY

EXECUTIVE SUMMARY

The National Cyber Security Division (NCSA) United States Computer Emergency Readiness Team (US-CERT) serves as a focal point for addressing cyber security incidents within the federal government. One of the primary functions of the US-CERT is the need to increase Government's awareness of cyber threats, vulnerabilities, and readiness in preparing for and responding to attacks.

This Concept of Operations (CONOPS) is provided as the foundation document for the organization and defines the US-CERT products and services available to its federal customers. It includes the inputs, processes and outputs of US-CERT enabling increased protection, analysis, response and recovery from cyber attacks.

This document comprises four main sections. The first section introduces the CONOPS and lays out the missions and functions for NCSA/US-CERT. The second section lays out the public and private sector inputs that are critical to the government's ability to prepare for, mitigate, respond to and recover from cyber attack. The third section lays out the analytical processes used by NCSA. The fourth section lists specific US-CERT products and services provided to federal Departments and agencies

FOR OFFICIAL USE ONLY

- ii -

Table of contents

| | | |
|----------|----------------------------------------------------------------------------------|----|
| 1 | Introduction..... | 1 |
| 1.1 | Purpose..... | 1 |
| 1.2 | Incident Handling Mission..... | 1 |
| 1.3 | Background..... | 2 |
| 1.4 | Authorities..... | 2 |
| 1.5 | Primary Functions..... | 2 |
| 2 | INFORMATION GATHERING (INPUTS)..... | 3 |
| 2.1 | Government..... | 3 |
| 2.1.1 | Federal Incident Response Teams (CERT, CSIRT, CSIRC)..... | 3 |
| 2.1.2 | Computer Network Defense Service Provider (CNDSP)..... | 3 |
| 2.1.3 | Law Enforcement..... | 3 |
| 2.1.4 | Intelligence Community..... | 3 |
| 2.1.5 | Other DHS Offices..... | 4 |
| 2.1.6 | State and Local Governments..... | 4 |
| 2.1.7 | Foreign Governments..... | 5 |
| 2.2 | Private Sector..... | 5 |
| 2.2.1 | Technology and Service Providers..... | 5 |
| 2.2.2 | Sector Coordinating Councils (SCC)..... | 5 |
| 3 | US-CERT OPERATIONS..... | 7 |
| 3.1 | Overview..... | 7 |
| 3.2 | Security Operations Centers (SOCs)..... | 7 |
| 3.3 | US-CERT Roles & Responsibilities..... | 7 |
| 3.4 | Shift Task List..... | 9 |
| 3.5 | Categories..... | 10 |
| 3.6 | Incident Reporting to US-CERT..... | 10 |
| 3.7 | Analysis of Agency Incident/Event Data..... | 15 |
| 3.8 | US-CERT Assignment of a Severity Rating..... | 16 |
| 3.9 | Communication During an Incident..... | 17 |
| 3.10 | US-CERT Products for Federal Agencies..... | 17 |
| 3.10.1 | US-CERT Response to Severity Levels..... | 18 |
| 3.10.1.1 | US-CERT Response to Severity Level 1 (Minimal) and Level 2 (low) Activities..... | 18 |
| 3.10.1.2 | US-CERT Response to Severity Level 3 (Medium) Activities..... | 18 |
| 3.10.1.3 | US-CERT Response to Severity Level 4 (High) Activities..... | 19 |
| 3.10.1.4 | US-CERT Response to Severity Level 5 (Crisis) Activities..... | 19 |
| 3.10.2 | Federal Information Notices (FIN)..... | 19 |
| 3.10.3 | Special Communications..... | 20 |
| 3.10.4 | US-CERT After Action Reports..... | 20 |
| 3.10.5 | Trends Analysis..... | 20 |
| 3.10.6 | On-site Incident Response Assistance to Agencies..... | 20 |
| 3.10.7 | Incident Escalation..... | 20 |
| 3.10.8 | Federal Agency Input (Feedback)..... | 21 |
| 4 | MALICIOUS CODE ANALYSIS PROGRAM..... | 22 |

FOR OFFICIAL USE ONLY

- iii -

| | | |
|-------|--------------------------------------------|----|
| 4.1 | Overview | 22 |
| 4.1.1 | Collection/Submission Program..... | 22 |
| 4.1.2 | Malicious Code Lab | 23 |
| 4.1.3 | Reports of Analysis Activity..... | 23 |
| 4.2 | Goal | 23 |
| 4.3 | Primary Objectives..... | 24 |
| 4.4 | Benefits..... | 24 |
| 4.5 | Interdependencies and Inputs | 24 |
| 4.6 | Deliverables/Products..... | 24 |
| 4.7 | Success Factors | 25 |
| 5 | EINSTEIN..... | 26 |
| 5.1 | Overview | 26 |
| 5.2 | Phased Approach..... | 27 |
| 5.3 | Technical Overview – Current Phase..... | 27 |
| 5.3 | Operational Capabilities and Benefits..... | 28 |
| 5.4 | Conclusion..... | 29 |
| A | HSIN/US-CERT PORTAL..... | 31 |
| A.1 | Overview | 31 |
| A.1.1 | Emerging Threat Forum | 31 |
| A.1.2 | Malware Code Analysis Forum | 31 |
| A.1.3 | Incident Response Forum | 31 |
| A.1.4 | Vulnerabilities Forum..... | 32 |
| B | CYBER FORENSICS TRAINING..... | 33 |
| B.1 | Overview | 33 |
| B.2 | Objectives | 33 |
| B.3 | Primary Benefits | 34 |
| C | CNDSP PROGRAM..... | 35 |
| C.1 | Overview | 35 |
| C.2 | Objectives | 35 |
| C.3 | Primary Benefits | 36 |
| D | GLOSSARY..... | 37 |

FOR OFFICIAL USE ONLY

1 Introduction

1.1 Purpose

This CONOPS focuses on Federal Cyber Security Incident Handling. This CONOPS defines the US-CERT products and services available to federal customers tasked with preventing, detecting and responding to cyber incidents at their agencies. The CONOPS is supported by the Standard Operating Procedures (SOPs) of the various organizations with which the US-CERT interacts as well as the following US-CERT Operational SOPs now in development. These SOPs will provide more detailed instruction on functions performed by US-CERT personnel in US-CERT interaction with various constituents. This document describes how the various mission components, constituents, and operations work to accomplish the US-CERT mission.

1.2 Incident Handling Mission

The National Strategy to Secure Cyberspace, Homeland Security Presidential Directives, National Security Presidential Directives, and Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets; recognizes the highly networked nature of the current Federal computing environment and provides effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; provides for development and maintenance of minimum controls required to protect Federal information and information systems; provides a mechanism for improved oversight of Federal agency information security programs; acknowledges that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and recognizes that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products. Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center US-CERT to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

FISMA, Section 3546 states that the Federal information security incident center, US-CERT, will perform the following functions:

- (1) Provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;
- (2) Compile and analyze information about incidents that threaten information security;
- (3) Inform operators of agency information systems about current and potential information security threats and vulnerabilities; and
- (4) Consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security

FOR OFFICIAL USE ONLY

Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

In accordance with Department of Defense (DoD) Directive O-8530-1, all DoD services and agencies are to report incidents to the Joint Task Force Global Network Operations (JTF-GNO), which will, in turn, coordinate directly with the US-CERT.

1.3 Background

NCSD was created in June 2003, as the nation's focal point for cyber security incorporating the roles and responsibilities of the Federal information security incident center. To promote cooperation and coordination between and among the government and the public and private sectors in the area of cyber security, the US-CERT was created in September 2003 as the operational arm of NCSD. US-CERT provides a federal capability that helps protect and maintain the continuity of our federal government.

1.4 Authorities

The NCSD/US-CERT operates under five key authorities, which are: 1) The National Strategy to Secure Cyberspace, 2) The Homeland Security Act of 2002, 3) The Federal Information Security Management Act (FISMA), 4) Homeland Security Presidential Directive 7 and 5) National Security Presidential Directive 38.

1.5 Primary Functions

To continuously assess threats and vulnerabilities to Federal, State and Local Government cyber systems, and reduce potential damage from such events, NCSD/US-CERT will perform strategic analysis, issue warnings/alerts, and coordinate response and recovery efforts.¹

¹ *The National Strategy to Secure Cyberspace*, Executive Summary, February 2003.

2 INFORMATION GATHERING (INPUTS)

US-CERT gathers information on federal cyber incidents from a variety of sources. US-CERT interacts with each of these groups in different capacities as deemed necessary by the reason and magnitude of the interaction. Interactions consist of two-way information sharing in the form of direct person-to-person interaction or documented products, to improve overall situational awareness.

2.1 Government

2.1.1 Federal Incident Response Teams (CERT, CSIRT, CSIRC)

US-CERT regularly collaborates with federal incident response teams across the federal civilian agencies and the Department of Defense. Government agencies may report suspected incidents via phone (1-888-282-0870), email (soc@us-cert.gov), secure email (us-cert@dhs.sgov.gov), the Homeland Security Information Network/US-CERT portal, or the US-CERT website (<http://www.us-cert/federal/>). This will ensure a central repository of federal incident data. Reporting helps to ensure that all incidents reported will be cataloged, indexed, and prioritized for analysis. To provide real-time direct incident support, US-CERT technical staff is available 24 hours a day 7 days a week to answer questions, provide technical assistance and receive reports of anomalous activity, virus infections or other forms of cyber attack.

Federal Incident Response Teams need to catalog their agency capabilities (i.e. forensic, malware, analytical, etc) and points of contact so that agencies can be leveraged appropriately in the event of a national level cyber incident. The US-CERT will be creating a federal agency directory of subject matter experts and teams points of contact for the purposes of the National Response Plan Cyber Annex and National Cyber Response Coordination Group. This directory will be updated on an annual basis.

2.1.2 Computer Network Defense Service Provider (CNDSP)

A CND Service Provider is a CND-capable resource that may help US-CERT in meeting defined requirements, either by providing additional resources integrated into US-CERT, or by providing reach-back resources. Specifically, A CNDSP can be staff augmentation (e.g. contractors in the watch/ops center) or it could be a vendor. A Computer Emergency or Incident Response Team (CERT/CSIRT/CSIRC) may provide computer network defense services commonly located within a Network Operations or Security Operations Center (NOC/SOC) or a private sector vendor. The CERT "services" are voluntary in that no contractual obligation exists to share data.

2.1.3 Law Enforcement

The US-CERT regularly collaborates with the law enforcement community to share information and coordinate analysis. NCSD has incorporated a law enforcement/intelligence component into its operations and leverages personnel from the US Secret Service and the National Security Agency in NCSD's Law Enforcement and Intelligence liaison division.

2.1.4 Intelligence Community

The Intelligence Community (IC) coordinates and shares information with US-CERT to safeguard the integrity of IC networks and support infrastructure protection across the

FOR OFFICIAL USE ONLY

government agencies and private sector infrastructure owners. US-CERT and the IC have established working groups in the area of attribution and botnets. The intelligence community also provides information on cyber foreign threats, recommended mitigations, and indicators of new vulnerabilities.

2.1.5 Other DHS Offices

The US-CERT Operations Center is a component of the DHS National Infrastructure Coordination Center (NICC). The US-CERT Operations Center coordinates information pertaining to cyber activities across the NICC and DHS Infrastructure Protection (DHS/IP) operations. The Office of Infrastructure Protection is the focal point for national infrastructure protection efforts across each of the critical infrastructure sectors, within the segments that comprise these sectors, and across the spectrum of assets including physical, people, and cyber assets. DHS/IP office is comprised of the Protective Service Division (PSD), National Communications System (NCS), Infrastructure Coordination Division (ICD), Strategic Partnership Office (SPO), and National Cyber Security Division (NCSD).

To coordinate efforts regarding both physical and cyber emerging threats and vulnerabilities the members of IP hold a combined watch teleconference daily. This conference call provides a forum for the participants to discuss and share pertinent information related to the protection and ongoing operations of the nation's critical infrastructures among the IP watch and analysis operations. Any information deemed actionable will be included in the Cyber Daily discussed below in more detail and would initiate a phone call from a member of the US-CERT operations team to affected parties to include but not limited to: government agencies, information sharing organizations, or private sector organization. This call does not serve as the sole interaction between the divisions and ad hoc communication is encouraged when deemed necessary. In addition to the daily conference call, all participants are active members of the Homeland Security Information Network (HSIN)/US-CERT portal, a secure portal that is available to share watch-related activities on a 24x7 basis.

The Homeland Security Operations Center (HSOC), located at the Nebraska Avenue Complex (NAC) is the operational focal point for the Secretary of the Department of Homeland Security on homeland security matters. The Interagency Incident Management Group (IIMG) convenes at the HSOC in case of an incident. The National Cyber Response Coordination Group (NCRCG) provides cyber security incident management and other information to the IIMG and HSOC as necessary.

The Information Analysis (DHS/IA) organization within DHS IAIP is responsible for intelligence community coordination and analysis as it relates to Homeland Security. US-CERT engages regularly with DHS/IA to ensure an accurate understanding of current and emerging cyber threat data from the intelligence community.

2.1.6 State and Local Governments

The US-CERT has engaged with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and a series of other key organizations, including the National Association of State Chief Information Officers (NASCIO), in order to better coordinate cyber cooperation and incident response through the HSIN/US-CERT Portal to allow for 24x7, real time interaction between and among federal and state and local governments.

FOR OFFICIAL USE ONLY

2.1.7 Foreign Governments

Establishing relationships, addressing common issues and enhancing coordination and cooperation with international partners are paramount to responding to the increasing cyber threat. The US-CERT actively engages with the interagency team on international efforts in multilateral organizations, regional activities, and bilateral partnerships. US-CERT receives international information, through the Global Watch Network, which is a virtual network between Australia, Canada, United Kingdom and United States government CERTs. Each country is responsible for providing an “end-of-shift” report resulting in around the clock coverage. Additional international sharing initiatives are under development and should be finalized by 2005, which will establish greater incident readiness, response, and cooperation globally.

2.2 Private Sector

Public-private engagement is a key component of securing the federal government’s cyberspace. Public-private partnerships can significantly enhance information exchange in the areas of awareness, software assurance, control system security, and incident preparedness, response, and recovery. Dozens of private companies with significant cyber watch and response capabilities are active members of the HSIN/US-CERT portal and working with US-CERT to improve the nation’s ability to prepare for, mitigate against, respond to, and recover from cyber attack.

In addition many private sector companies have established organizational watch and warning centers. These functions may manifest themselves as security operations centers, network operations centers or CERTs. The premise and intent for their operations, however, is quite similar – ensure connectivity and security of the respective networks. The US-CERT works closely with operators of these entities to ensure accurate, up-to-date information on cyber security threats and vulnerabilities.

2.2.1 Technology and Service Providers

These groups are the foundation to the long-term protection and securing of cyberspace as they produce new and more secure technologies, implement those technologies more quickly, and produce current technologies in a more secure way. Commercial ISPs provide Internet connectivity for both the government and the private sector and therefore require close coordination and collaboration between them and US-CERT for awareness purposes and possible engagement in response and recovery efforts during time of major incident. These groups understand they have a responsibility to safeguard critical IT assets, both those that serve their respective sector itself and the IT products and services deployed in other industry sectors. As such, products and services need to account for the ever-changing technology environment as well as the associated threats and vulnerabilities.

2.2.2 Sector Coordinating Councils (SCC)

The means of partnering with sector stakeholders is evolving as each sector becomes better defined. Prior to the creation of DHS, an architecture consisting of Sector Coordinators and Information Sharing and Analysis Centers (ISACs) was created to form this partnership, which achieved many early successes. With the creation of DHS and the development of the National Infrastructure Protection Plan (NIPP), this partnership must evolve to meet new requirements for enhanced capabilities and a revised framework.

FOR OFFICIAL USE ONLY

Sector Coordinating Councils bring together the entire range of infrastructure protection activities and issues to a single entity. Sector Coordinating Councils are private sector coordinating mechanisms that comprise private sector infrastructure owners and operators and supporting associations, as appropriate. One role of the Sector Coordinating Councils is to identify or establish and support the information sharing mechanisms that are most effective for their sector, drawing on existing mechanisms, such as ISACs or creating new means as required.

ISACs gather information on vulnerabilities, threats, intrusions, and anomalies from their respective industry, government, and other sources, and analyze the data with the goal of averting or mitigating impact upon the respective infrastructure. Additionally, data is used to establish baseline statistics and patterns and maintained to provide a library of historical data. Results are sanitized and disseminated in accordance with sharing agreements established for that purpose by the ISAC participants. This information in aggregate will be shared with federal sector lead agencies and the Government Forum of Incident Response Teams to highlight cyber event or incident trends in specific or multiple sectors that could impact federal agencies.

FOR OFFICIAL USE ONLY

3 US-CERT OPERATIONS

3.1 Overview

US-CERT must combine the right mix of people, processes and technology to produce a sufficient level of technological expertise in order to instantly and accurately analyze new or evolving security events. The success or failure of the US-CERT Operations Center depends significantly on how accurate the US-CERT security analysts judge the severity as security events emerge. US-CERT is staffed through multiple contracting agencies and government employees. Moreover, US-CERT Operations Center maintains active partnerships with key organizations that can provide the necessary cyber security expertise to assist US-CERT personnel.

3.2 Security Operations Centers (SOCs)

US-CERT operates two SOC's 24 hours per day, 7 days per week, 365 days per year (24 x 7 x 365) that are operated from two different locations; 1110 North Glebe Road, Arlington, Virginia 22201 - 9th Floor and DHS Nebraska Avenue Complex HSOC. Authorization to access the US-CERT at either location is by approval of the DHS Security Officer. US-CERT analysts' work structured shifts to facilitate operations. Shift changes occur in eight, ten, or thirteen-hour increments.

3.3 US-CERT ROLES & RESPONSIBILITIES

The roles and responsibilities of the US-CERT staff are shown below:

Table 3-1 Roles and Responsibilities of US-CERT Staff

| Role | Responsibilities in US-CERT Operations |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| US-CERT Analyst | <ul style="list-style-type: none"> • Responds to intrusion attempts, malicious logic incidents and physical threats. • Opens, resolves, and closes US-CERT trouble tickets, when necessary. • Analyzes, coordinates and responds to technically complex incidents and threats to IT systems across the Federal government. • Enters incident data into US-CERT database. • Provides guidance and support to Federal agencies responsible for network or computer security operations to ensure that incident response is aligned with federally mandated security practices. • Recommends effective countermeasures or actions to be taken during an incident or attack. • Assists Federal agencies in investigation and resolution of computer incidents. |

FOR OFFICIAL USE ONLY

| Role | Responsibilities in US-CERT Operations |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| US-CERT Shift Lead | <ul style="list-style-type: none"> • Performs work listed under US-CERT Analyst. • Monitors and is responsible for activities that occur throughout assigned shift. • Performs shift turnover meeting in accordance with documented shift turnover procedures. • Manages ongoing tasks and current shift assignments as dictated by the US-CERT Technical Lead or US-CERT Operations Lead. • Trains new Analysts on assigned shift. |
| US-CERT Technical Lead | <ul style="list-style-type: none"> • Performs work listed under US-CERT Analyst. • Develops plans for on-going US-CERT activity. • Helps inventory government and other-furnished equipment and software. • Interacts as required on items of highest exposure and risk. • Notifies NCSA Secret Service Liaison of potential criminal activity, turning over potential evidence, providing resistance algorithms and containment approaches for attacks. • Gives direction to US-CERT Team for specific activity that will lead to fair, equitable, effective, and structured distribution of work. • Writes procedures and processes for performing incident detection and response activities. • Provides feedback and lessons learned to the US-CERT. |
| US-CERT Operations Lead | <ul style="list-style-type: none"> • Oversees security incident response operations. • Checks that commitments made by US-CERT staff to the US-CERT are carried out in an efficient and excellent manner. • Assures consistent and detailed incident response for users of US-CERT. • Keeps a software and hardware inventory. • Catalogs, writes, and maintains security processes and procedures. • Writes project plans for significant activities. • Tracks and verifies completion of incident tickets, security advisories, and information reported during daily conference calls. |
| US-CERT Architect | <ul style="list-style-type: none"> • Performs work listed under US-CERT Analyst. • Interfaces and interacts with US-CERT Situational Awareness and Tools. • Develops security architectures considering network, firewall, IDS, and workstation implications. • Reviews proposed IT Architectures that contain security components. • Develops CM guidelines and processes for use and inventory of security components. • Ensures compliance to Department of Homeland Security and NIST guidelines and policies for Security Components. • Provides long-term plans for IT and Security Architecture. |
| US-CERT Project Manager (PM) | <ul style="list-style-type: none"> • Responsible for conduct of the contracts for US-CERT work. • Reports contract status to US-CERT COTR and management. • Generates and delivers status reports to the US-CERT. • Responsible for overall management, hiring, salary, and performance of contracts and their subcontractors. • Manages effort and cost for contracts and reports potential or real deviations to contracted norms. |

FOR OFFICIAL USE ONLY

| Role | Responsibilities in US-CERT Operations |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| US-CERT | |
| Deputy Director, Operations | <ul style="list-style-type: none"> Responsible for all proactive and reactive activities to assure the proper security measures are implemented at the US-CERT. Has approval authority on unplanned security incidents pursued. Point of Contact for US-CERT: channels activities to appropriate US-CERT internal resources. |
| US-CERT Operations Manager | <ul style="list-style-type: none"> Makes decisions about whether operations can be impacted by updates or other downtime experienced in the system (i.e., unplanned changes). Provides information to US-CERT about impact on operations of incidents. |

3.4 Shift Task List

In addition to recording and prioritizing all reported incidents and events, US-CERT personnel are responsible for completing a general set of tasks during their assigned shifts. The table below shows a consolidated list of tasks that are performed.

Table 3-2 Shift Task List of US-CERT Staff

| Task | Source | Execute Time or Event | Procedure |
|----------------------------------------|--------------------------------|-----------------------|-----------|
| Conduct Shift Turnover Meeting | Artifacts from Departing Shift | Beginning of Shift | |
| Review Shift Change Log | Shift Change Log | Beginning of Shift | |
| Write Shift Change Log | Shift Change Log | End of Shift | |
| Check Soc Email | Lotus Notes | Continuous | |
| Process Tickets | Email, Telephone, Website, Fax | Continuous | |
| Conduct EINSTEIN Analysis | EINSTEIN | Continuous | |
| | Other Tools | Continuous | |
| 0900 Phone Conference | Telephone | Monday-Friday | |
| | | | |
| Monitor CNN | Cable/Satellite | Continuous | |
| Receive/Report Cyber Incident/Analysis | Email | Continuous | |

FOR OFFICIAL USE ONLY

| Task | Source | Execute Time or Event | Procedure |
|---------------------------------------------------------------|------------------|-----------------------------------------------------------|-----------|
| 1100 Phone Conference | Telephone | Monday-Friday | |
| Physical Security Checks | Facility | TBD | |
| Flash Report Input | US-CERT Database | 12:00 p.m. each Tuesday | |
| Write/Distribute Monthly Incident Reports to Federal Agencies | US-CERT Database | Last Day of Each Month | |
| CWIN Phone Conference | STE Telephone | Tuesday, Thursday, Saturday | |
| Review Cyber Intel Reports | Classified LAN | 12:00pm Daily | |
| Write and Distribute last 24 hour Report | Multiple Sources | 6:00 a.m. Daily to US-CERT Deputy Director via DHS E-mail | |

Assigned shift leads are responsible for ensuring that the aforementioned tasks are completed prior to the shift ending. Detailed procedures for completing these tasks are outlined in the various US-CERT SOPs.

3.5 Categories

A computer incident within the federal government as defined by NIST Special Publication 800-61 is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In order to clearly communicate incidents and events (any observable occurrence in a network or system) throughout the Federal Government and supported organizations it is necessary for the government incident response teams to adopt a common set of terms and relationships between those terms. All elements of the federal government should use a common taxonomy. Below please find a high level set of concepts and descriptions to enable improved communications among and between agencies. The taxonomy below does not replace discipline (technical, operational, intelligence) that needs to occur to defend federal agency computers/networks, but provides a common platform to execute the US-CERT mission. In certain instances incident categories will contain sub-categories to enable further granularity in reporting. For example, Category 3; Malicious code will further break into sub-groups to identify and include virus, worm, botnet and spyware. Further, Category 5; Scans, Probes, Attempted Access will include the ability to specify network scans, phishing attempts, and pharming attempts.

US-CERT and the federal civilian agencies are to utilize the following incident and event categories and reporting timeframe criteria as the federal agency reporting taxonomy.

FOR OFFICIAL USE ONLY

Table 3-3 Federal Agency Incident Categories
***Defined by NIST Special Publication 800-61**

| CATEGORY | NAME | DESCRIPTION | REPORTING TIMEFRAME |
|----------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| CAT 0 | Exercise/Network Defense Testing | This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses. | Not Applicable; this category is for each agency's internal use during exercises. |
| CAT 1 | *Unauthorized Access | In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource. | Within one (1) hour of discovery/detection. |
| CAT 2 | *Denial of Service (DoS) | An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. | Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity. |
| CAT 3 | *Malicious Code | <i>Successful</i> installation of malicious software (i.e. virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software. | Daily Note: Within one (1) hour of discovery/detection <i>if</i> widespread across agency. |
| CAT 4 | *Improper Usage | A person violates acceptable computing use policies | Weekly |

Table 3-4 Federal Agency Event Categories

| CATEGORY | NAME | DESCRIPTION | REPORTING TIMEFRAME |
|----------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| CAT 5 | Scans/Probes/Attempted Access | This category includes an activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. | Monthly Note: If system is classified, report within one (1) hour of discovery. |
| CAT 6 | Investigation | <i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. | Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated. |

To ensure a consistent means of reporting and trending of security events across the Federal Government, the following are offered as examples of each Category:

Category 0: Exercise/Network Defense Testing

FOR OFFICIAL USE ONLY

- Federal agency and the US-CERT are participating in a National level exercise to gauge cyber preparedness and in order to simulate a 'real world' situation, initiates communication with US-CERT.

Category 1: Unauthorized Access

- Federal agency reports a critical system has a suspicious and unknown user account with Administrator privileges. Agency has isolated the vector of attack to an unauthorized remote access tool that an attacker installs via unsecured network shares.
- Federal agency reports that a publicly available exploit tool has been used to create a back door account on a public web server.

Category 2: Denial of Service (DOS)

- Federal agency reports a concentrated denial of service against a production mail server. The attack prohibited the agency from sending or receiving email until the attack subsided.
- Federal agency reports a router mis-configuration has enabled an attacker to use the agency network to participate in a reflective denial of service attack against a commercial company. While the attack does not hinder network connectivity for the agency, the involvement in a denial of service attack merits this event being reported as a Category 2.

Category 3: Malicious Code

- Federal agency reports an outbreak of a previously known virus on their network.
- Federal agency reports that a bot network has been discovered on several internal machines.
- Federal agency reports that multiple desktop machines were discovered running a malicious spyware program. User's private information was being collected and sent to an outside third party.
- Federal agency reports that a user unintentionally clicked on a suspicious executable, which then activated a worm outbreak on the network.

Category 4: Improper Usage

- Federal agency reports that a user, in violation of the agency's acceptable use policy, has installed a peer to peer program to download music and video files.
- Federal agency reports that a user has used agency systems to view inappropriate content.

Category 5: Scans/Probes/Attempted Access

- Federal agency reports that multiple systems have been the subject of intense scanning and that various exploit attempts have been initiated against their systems from the same source IP address. Systems are not compromised.
- Federal agency reports that a user received a fraudulent phishing email which directed the employee to visit an external web site and input sensitive employee information. The user unwittingly visited the web site, however did not input any information.

Category 6: Investigation

FOR OFFICIAL USE ONLY

- Federal agency reports suspicious network traffic pattern destined for a system located external to the organization. While the agency suspects a system compromise, they have not identified the source of the traffic.
- Federal Agency reports unusual system behavior from a development web server. Agency is performing an internal investigation to determine cause of behavior.

3.6 Incident Reporting to US-CERT

Reports shall be transmitted in a manner consistent with their sensitivity and source network classification. Sensitive But Unclassified (SBU) reports can be submitted directly to the US-CERT via one of the following methods:

| | |
|-----------|-------------------------------------------------------------------------------|
| EMAIL | soc@us-cert.gov* |
| WEBPAGE | http://www.us-cert.gov/federal/ |
| PORTAL | https://gfirst.us-cert.gov |
| TELEPHONE | 888-282-0870 |
| FAX | 703-235-5963** |

*US-CERT can send and receive encrypted email utilizing Pretty Good Privacy (PGP)

**Please call and notify US-CERT Operations prior to the fax is being transmitted.

Classified network reports at the *SECRET* level can be submitted to the US-CERT via the following methods:

| | |
|-------------------|------------------|
| EMAIL | us-cert@dhs.gov* |
| STE/STU-III | 703-235-5043* |
| CLASSIFIED FAX | 703-235-5043* |

*US-CERT Operations can only communicate and store up to *SECRET* on-site at this time.

Reports shall include a description about the incident or event and as much of the information listed below as possible; however, reporting should not be delayed in order to gain additional information:

- ✓ Agency name
- ✓ Point of Contact Information (name, telephone, email)
- ✓ Incident Category Type (CAT 1/2/etc)
- ✓ Incident date/time (Timezone)
- ✓ Source IP, Port, Protocol
- ✓ Destination IP, Port, Protocol
- ✓ Operating System and version, patch, etc.
- ✓ System Function (DNS/Web server, workstation, etc)
- ✓ Antivirus software installed, version, latest update
- ✓ Location of the system(s) involved in the incident (Washington DC, Los Angeles, CA)

FOR OFFICIAL USE ONLY

- ✓ How was the incident identified (IDS, audit log analysis, system administrator)
- ✓ Impact to agency
- ✓ Resolution

Using the above information all reports to the US-CERT will be submitted utilizing the reporting matrix located in (Figure 3-1) below. All incident response teams will utilize this schema when reporting incidents to the US-CERT. Depending on the criticality it is not always feasible to gather all the information prior to reporting, but to continue to report information as it is collected.

FOR OFFICIAL USE ONLY



Homeland
Security

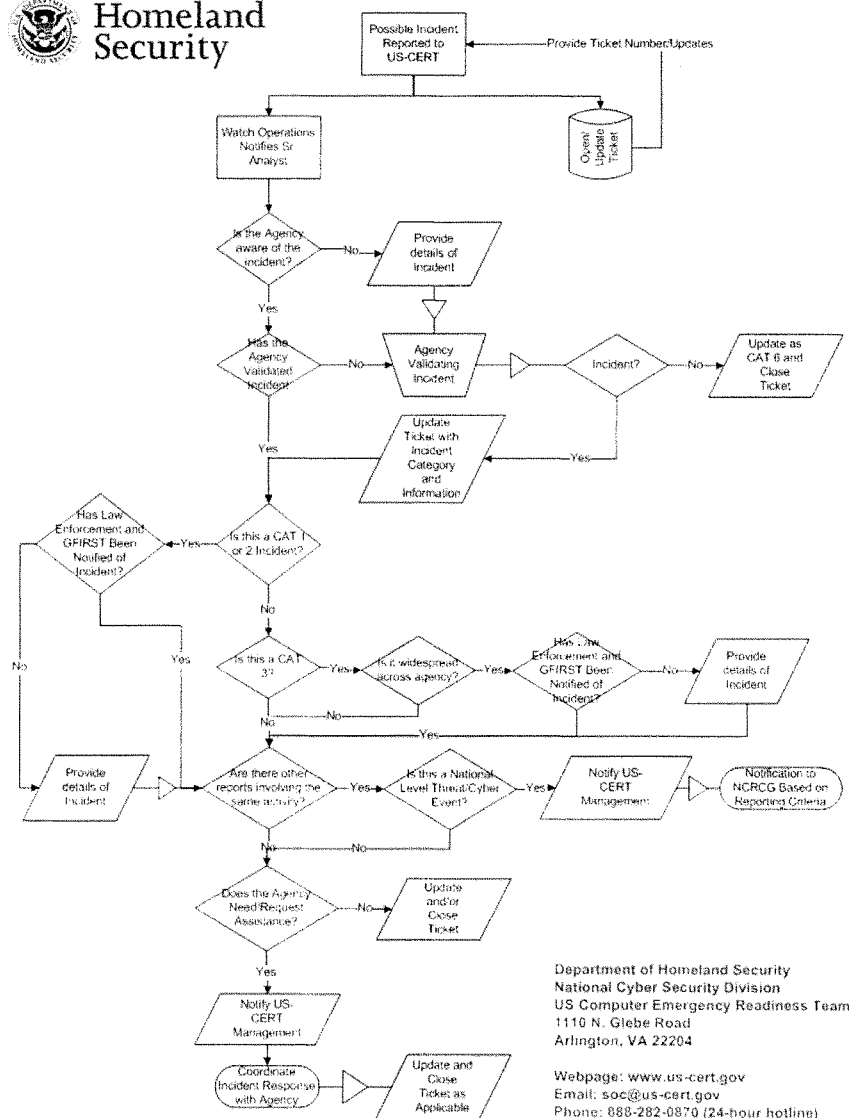


Figure 3-1 Federal Agency Reporting Matrix

3.7 Analysis of Agency Incident/Event Data

FOR OFFICIAL USE ONLY

Once information is received as discussed above it is analyzed in-house based on US-CERT best practices, technical tools, defined processes and procedures and considered for dissemination throughout a series of US-CERT products. All government agency reports of incidents and events received are triaged and reviewed upon receipt. Upon confirmation of incidents or events having a high severity rating, the US-CERT will directly communicate to the reporting agency as well as all affected agencies to provide a status update and suggested mitigation or response activities.

3.8 US-CERT Assignment of a Severity Rating

US-CERT uses a standardized, repeatable and reliable method to assess the criticality or severity of a new or emerging cyber security event. The initial step after gathering information is to assess its “severity” using a scale from 1 to 5, with 1 being minimal and 5 being a crisis. Factors that are weighed in determining the ‘severity’ of a security event are based upon the following matrix:

Table 3-5 Severity Table

| Vulnerability | Exploit | Emerging Threat |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Is the vulnerability widely known? ² | Method & speed of propagation | Is the threat unique? |
| Is exploitation of the vulnerability being reported to incident response? | Protocol & ports | Does current anti-virus signatures detect the threat (are anti-virus vendors developing new signatures to protect against the threat?) |
| Is the Internet infrastructure at risk? | Payload; how destructive is it? | Is this repetitive of prior attacks? |
| What is the number of Internet systems at risk? | How many units are known to be affected? | Overall impact to the Internet community |
| What is the impact on users of exploiting the vulnerability? | Relatively speaking, how important are the systems affected? | Visibility in the press |
| How easy is it to exploit the vulnerability? | How many unique sites or reporters have informed us of this activity? | See also the factors for Exploit. |
| What is the previous access required to exploit? | What is the localized impact of this activity during the incident? | |
| Visibility in the press | What is the residual impact of this activity after the incident? | |
| | How complicated is the attack method | |
| | Visibility in the press | |

This assessment methodology is progressive. When relevant information is received concerning a unique security event or incident, its severity rating is assigned or reassessed with the receipt of updated or new information as the event progresses. The nature of the information and its severity rating dictates the actions taken by US CERT.

² The discovery of a new vulnerability known only to a select few individuals necessitates a very careful review by the US-CERT Operation Center regarding the potential individual or groups to whom that information may be shared.

Table 3-6 Severity Rating

| Severity | Rating | Description |
|----------|--------|--------------------------------------------------------------------------------|
| Minimal | 1 | Negligible impact on the federal government. |
| Low | 2 | Very low impact on the federal government. |
| Medium | 3 | Poses a potential impact on the federal government. |
| High | 4 | Has impacted the federal government. |
| Crisis | 5 | Has had a severe impact on the operational capacity of the federal government. |

3.9 Communication During an Incident

To ensure constant communication during an incident, US-CERT will reach out to a reporting agency within 24 hours if no other direct communication through email, phone or the portal has been made. This will help to ensure all information is current and accurate. This 24-hour cycle will continue through the extent of an incident during the first 2 weeks. For long-term incidents a process will be arranged between US-CERT and the affected agency to ensure that on-going communication between agency and US-CERT is maintained as necessary.

Once an incident has been resolved, it essential that agencies notify and update the US-CERT so that the ticket can be closed. This notification should be made through email or phone within 24 hours of resolution. Once an incident is closed out, US-CERT will update the tracking system and archive the incident for future reference as needed.

3.10 US-CERT Products for Federal Agencies

At the heart of US CERT's mission is the need to share, on a real-time basis, relevant cyber security information with the federal agencies. The final state of the incident management process is dissemination. Once the information is received and analyzed, US-CERT employs a progressive response system based upon the severity rating.

All products are released as soon as possible, based on resource availability. As appropriate, US-CERT collaborates with partners, through the HSIN/US-CERT Portal and direct person-to-person interaction prior to release.

Table 3-7 Severity – Response Matrix

| Potential Responses to Emerging Cyber Security Events | Severity Rating | | | | |
|----------------------------------------------------------------------|-----------------|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Cyber Daily Update | | | | | |
| Update Current Activity | | | | | |
| Update Vulnerability Cards in Knowledge Base | | | | | |
| Issue Vulnerability Note | | | | | |
| Create specific forum on Portal | | | | | |
| Issue Special Communication | | | | | |
| Notification to Portal Users (e.g., CISO Forum, CIIMG, GFIRST, etc.) | | | | | |
| Direct outreach to potential affected/targeted groups | | | | | |
| Outreach to others in Private Sector | | | | | |
| Intel/LE Information Sharing | | | | | |
| International Information Sharing | | | | | |
| National Cyber Alert System | | | | | |

| | |
|--|-------------------------------------------------------|
| | NCSD will take No Action |
| | NCSD May Take the Potential Response |
| | NCSD will take one or more of the Potential Responses |

3.10.1 US-CERT Response to Severity Levels

3.10.1.1 US-CERT Response to Severity Level 1 (Minimal) and Level 2 (low) Activities

To provide federal agencies with a synopsis of the state of the Internet over a 24-hour period the US-CERT established a “Cyber Daily” report. The report contains vulnerability information and non-attribution unclassified incident information from both the federal and private sectors. The Cyber Daily can be reviewed by logging into the US-CERT Portal.

An incident or vulnerability may be included into the “Cyber Daily” and labeled as a severity level 1 or severity level 2, but no further response by US-CERT or the portal users is required. A minimal event will not elevate any direct activity from US-CERT and therefore agencies are expected to regularly read the “Cyber Daily” to ensure they are aware emerging threats and vulnerabilities.

3.10.1.2 US-CERT Response to Severity Level 3 (Medium) Activities

The event is included into the “Cyber Daily” which is published each day, updated throughout the day as necessary and labeled as a severity rating level 3. US-CERT staff would establish a new thread through the portal in the appropriate forum discussed above, to encourage dialogue between members to increase overall awareness.

FOR OFFICIAL USE ONLY

US-CERT will track the threat and will alert affected government agencies directly of the situation and will provide a series of mitigation or remediation strategies for possible implementation. Agencies are expected to relay relevant information surrounding the activity in question to affected stakeholders, keep an eye for suspicious activity and report any unusual activity to US-CERT.

3.10.1.3 US-CERT Response to Severity Level 4 (High) Activities

US-CERT and other first responder teams will need to take action to recover from incidents, or will need to take action to prevent compromise. US-CERT will perform all activities described above and will also directly reach out to all affected agencies within 1 hour of confirmation to provide appropriate coordination, response, or mitigation activities. Agencies are expected to relay relevant information to affected stakeholders so that they can institute protective measures, monitor for suspicious activity and report any unusual activity to US-CERT.

US-CERT will coordinate a conference call of members of the Government Forum for Incident Response and Security Teams (GFIRST), the Chief Information Security Officer's (CISO) Forum, or the Chief Information Officers (CIO) Council to alert members of specific threat information and necessary response activities. Agencies will also be asked to report back to US-CERT when they have completed mitigation/response activities.

As necessary, GFIRST members will convene as a group via conference call to discuss the emerging situation and discuss response activities. US-CERT will keep the conference call line open until resolution has been reached in responding or recovering to the cyber event so that teams can provide near real time updates on impact or pertinent information related to the incident. The group has collaborated more than 25 times during its first year to provide technical analysis of ongoing cyber activities. On at least 4 occasions the group has worked together to identify previously unseen/unidentified cyber events.

3.10.1.4 US-CERT Response to Severity Level 5 (Crisis) Activities

US-CERT will perform all response activities described above and will also notify members of the NCRCG, a forum of principle government agencies that coordinates intra-governmental and public-private preparedness and operations to respond to and recover from national level cyber incidents and physical attacks that have significant cyber consequences. NCRCG will provide a strategic picture of the impact to the information infrastructure and a coordinated response. The NCRCG will ensure that appropriate federal capabilities are fully leveraged and deployed in a coordinated effort. Additional information can be found in the NCRCG CONOPS. US-CERT will continue to work with the federal incident response teams, Office of Management and Budget (OMB), CIO, CISO, law enforcement, intelligence community, and the public and private sector to assess the situation and continually update the NCRCG as appropriate. This direct interaction helps to ensure that all agencies are aware of the situation and working on the same set of facts and assumptions.

3.10.2 Federal Information Notices (FIN)

US-CERT established the Federal Information Notice (FIN) to provide early warnings of Internet security problems exclusively to the federal incident response teams and offer explanations of potential problems that have not yet become serious enough to warrant an alert. The FIN does not replace any other US-CERT product; rather it is to be used in conjunction with them to add additional guidance and information. The FIN is released, regardless of level and/or impact of

FOR OFFICIAL USE ONLY

the incident to all members of the federal mailing list upon confirmation of the same incident being reported by three unique government agencies.

3.10.3 Special Communications

The US-CERT provides Special Communication e-mails to members of the GFIRST. Special Communications are informal documents, written by technical staff for technical staff, covering topics of current interest or special concern. US-CERT will often use this communication to preview draft publications, distribute preliminary analyses, or share information privately that is not intended for public distribution. Special Communications are released roughly 70 times per year.

3.10.4 US-CERT After Action Reports

At the conclusion of a severity level four or higher cyber event, US-CERT will pull together those that were involved in the incident within twenty-four hours for an initial meeting to walk through the timeline of events and actions taken so that a more detailed after action meeting can be held within thirty days of the cyber event. The purpose for this meeting is to conduct a detailed review of how the incident could have been prevented, a review of the response & recovery, and what the impact was. A final report will be developed from this working group and presented to all agencies involved so that actions might be taken to prevent or decrease the amount of time it takes to recover from another incident. A copy of the report will be sent to Office of the Vice President, Office of Management & Budget, Homeland Security Council and National Security Council. Also NIST & US-CERT published best practices will be reviewed to see where there might be opportunities to improve upon them or to publish new guidance on prevention, detection, and recovery efforts for a particular cyber incident that had substantial impact.

3.10.5 Trends Analysis

US-CERT will provide federal agencies with analysis of incident trends on a quarterly basis including an annual report that will be provided to incident response teams, Chief Information Security Officers, Chief Information Officers, Office of the Vice President, Office of Management & Budget, Homeland Security Council, and the National Security Council.

3.10.6 On-site Incident Response Assistance to Agencies

As needed, US-CERT will provide on-site response coordination and support to agencies without a 24x7 operations team and the necessary level of personnel. Based on the time and support required, US-CERT reserves the right to charge agencies on a fee for service basis to recover from costs associated with agency specific response activities.

3.10.7 Incident Escalation

Escalation criteria are based on actual operational incident reports received and analysis performed by the US-CERT. These criteria will indicate an incident that has operational significance through out the federal community. US-CERT has responsibility for maintaining and updating the list below and for publishing updates to reporting agencies as necessary. Factors are weighed and verified in determining the severity of an incident based upon the following criteria:

FOR OFFICIAL USE ONLY

Table 3-6 Escalation Criteria

| Escalation Criteria |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Any intrusion into a classified network. |
| Any unauthorized privileged user, administrator, or root level access of a system which crosses federal agency boundaries. |
| Any incident involving a second level domain name server. |
| Any incident which impacts a federal agency's operations. |
| Any incident from a country against which the US is currently conducting operations or will imminently conduct operations. |
| Any targeted intrusion of the Whitehouse networks. |
| Any incident involving a second level domain web server (e.g., www.dhs.gov, www.whitehouse.gov, etc.). |
| Any new virus/worm for which no published countermeasure exists, any new virus/worm whose propagation could likely circumvent federal agency containment capabilities, or any new virus/worm which affects vital network services (e.g., e-mail and DNS services). |
| Any root level access on a system using new methods, which exploit significant vulnerabilities shared across federal agency systems. |

US-CERT will continue to work directly with the federal incident response teams that include OMB, CIO, CISO, GFIRST, law enforcement, intelligence community, and the public and private sector to assess the situation and continually update all parties as appropriate.

In addition, US-CERT will notify members of the NCRCG, a forum of 13 principle federal agencies that coordinates intra-governmental and public-private preparedness and operations to respond to and recover from national level cyber incidents and physical attacks that have significant cyber consequences. This direct interaction helps to ensure that all agencies are aware of the situation and working on the same set of facts and assumptions.

Some of these organizations will need to know an incident occurred and what its potential operational impact is at the national level, if any. While other organizations will require more technical detail, to help them better protect their information assets for which they are responsible.

3.10.8 Federal Agency Input (Feedback)

US-CERT created the Chief Information Security Officer (CISO) Forum to provide a trusted venue for CISOs to collaborate and share effective practices, initiatives, lessons learned and discuss particularly problematic or challenging areas in a trusted environment. The CISO Forum meets in plenary sessions quarterly and holds separate working group meetings in the interim on an as-needed basis. One working group is focused on Incident Reporting, Response, and Management.

FOR OFFICIAL USE ONLY

4 MALICIOUS CODE ANALYSIS PROGRAM

4.1 Overview

A key component of the US-CERT's effort is the Malicious Code Analysis Program. Malicious code (e.g., viruses, worms, spyware, bots, trojan horses, and rootkits), other forms of attack tools, and the vulnerabilities exploited when attacks occur present a real and present danger to the security of U.S. information systems. Understanding the complete behavior of malicious code and other attack tools is imperative to developing countermeasures or recommending courses of action. To this end, the US-CERT works closely with cyber security experts in the federal government, intelligence community, public and private sectors. Detailed analysis of attack techniques and their impact to vulnerabilities allows for improved response times and the ability to mitigate potential future risks. As an enhanced benefit, this information assists law enforcement personnel in their efforts to identify the individual or individuals responsible for production, modification, or distribution of malicious code. The US-CERT Malicious Code Program includes the following elements.

4.1.1 Collection/Submission Program

Malicious code identified during the course of forensic type analysis involving compromised systems and malicious code in general deemed non detectable by current and updated anti-virus programs shall be sent to the US-CERT for further review. The malicious code analysis program within the US-CERT has developed procedures for the safe collection and transmission of samples to the US-CERT for analysis. To achieve this, agencies will need to submit these samples to the US-CERT in the proper format. After all related binaries are identified, compress the files into an archive (.zip or .rar format) and password protect the archive with the password "infected" (all lowercase without quotes). Lastly, the resultant file should be renamed to an ".usc" extension. The agency will then send the compressed, password protected, renamed file to the following US-CERT email address for review: virus-submit@us-cert.gov

Agencies submitting a properly formatted file will be notified by the US-CERT identifying their submission with a specific ticket number assigned to their submission, and the results of a multi-vendor anti-virus scan ran against the malicious code in question. In this manner agencies will be able to ascertain if their submission was not detected by more than one type of antivirus software, or perhaps if their vendor does not yet detect the malicious code in question. Malicious code sent to the US-CERT that does not meet the submission criteria detailed above will be quarantined by the US-CERT. Agencies having technical difficulties or questions about the submission program should contact the US-CERT directly for further guidance.

The malicious code files in question will be made available to the larger malicious code analysis community and to first responders as a means to safely and securely exchange information on possible malicious code, unless otherwise directed. In addition, these samples will be combined into a single repository for use in comparative analysis. Additionally, the US-CERT will utilize all practical means to collect and analyze suspect code using available in-house capabilities.

FOR OFFICIAL USE ONLY

Below (Figure 4-1) is a flowchart that depicts how the US-CERT Malicious Code Collection/Submission Program will work.

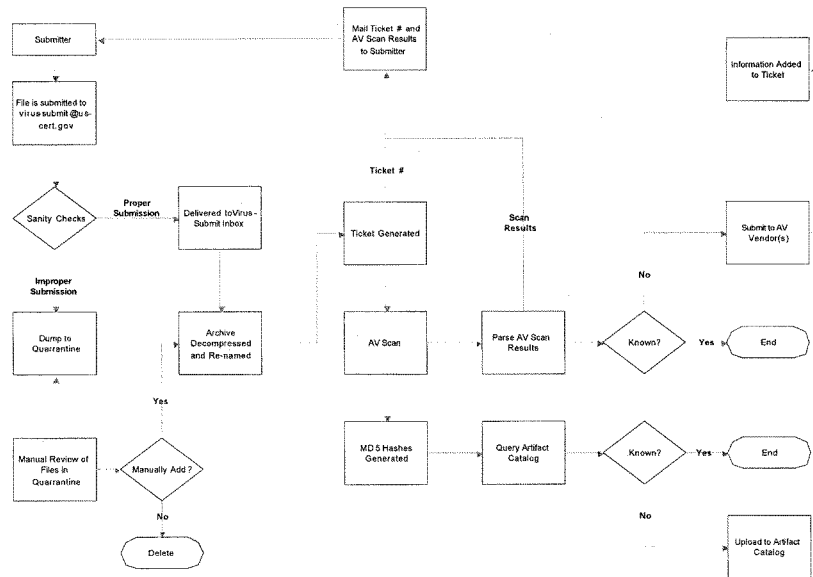


Figure 4-1 US-CERT Malicious Code Collection/Submission Program

4.1.2 Malicious Code Lab

The malicious code analysis activity comprises a laboratory function that analyzes malicious code and vulnerabilities and evaluates and develops counter measures. This function analyzes software to understand the potential impacts of malicious code, analyzes weaknesses in software that permit malicious code to operate, and supports collaboration with peer groups (particularly US-CERT) doing similar work. Finally, it disseminates the analysis results to public and private sector partners.

4.1.3 Reports of Analysis Activity

The malicious code analysis program will develop analysis reports aimed at informing the response community about tools, techniques and post-mortem analysis of dissected malicious code. These reports will focus on providing warning of impending threat, behavioral information, protective measures, recovery procedures, and other course of action recommendations.

4.2 Goal

To develop an in-house capability at the US-CERT to analyze malicious code to improve overall understanding of current or emerging cyber threats. The US-CERT will become a premier

FOR OFFICIAL USE ONLY

capability for the timely analysis of suspected malicious code and the production of actionable intelligence to aid incident response efforts.

4.3 Primary Objectives

- Develop procedures for the safe and secure handling of malicious code samples in a manner consistent with chain-of-evidence
- Create the means to collect suspect code to facilitate investigation of samples
- Maintain a streamlined capability to produce immediate actionable information, allowing for more detail as additional facts emerge
- Build a malicious code analysis lab to enhance analysis efforts and allow a more robust environment for the dissection of malicious code and the cataloging of related information
- Produce detailed reports of analysis activity for the purpose of informing and educating response personnel

4.4 Benefits

- Increased awareness in the incident response community of the threat of malicious code
- Timely and actionable information regarding emerging threats
- Coordinated effort within community will speed analysis and remediation

4.5 Interdependencies and Inputs

US-CERT malicious code analysis will rely on close ties with other malicious code capabilities, as well as with other US-CERT capabilities such as the forensics capability, to acquire samples of malicious artifacts for examination.

Information on malicious code may come in the form of notifications to the US-CERT operations center identifying Internet locations where code may be found, actual submissions of sample code for analysis, interactions with external entities, or the collection efforts of the US-CERT team.

4.6 Deliverables/Products

The US-CERT will:

- maintain a repository of malicious code samples and associated information for the purpose of cataloging and comparative analysis;
- maintain a database tracking malicious actors by pseudonym, relationally linked by behavior, group affiliation and other identifiable characteristics;
- develop preventive and protective measures for use in the defense of systems and response to incidents. These measures include, but are not limited to, IDS signatures, access control lists (ACLs), firewall rules and other suitable actions;
- identify and report characteristics unique to various pieces of malicious code that might be used in the determination of origin, intent or motivation for the creation of such code;
- report on new and novel attack techniques used in the exploitation of systems;
- report on malicious code found in the wild to promote awareness and encourage appropriate action;
- work with the community to develop tools and techniques to nullify the effects of exploits as they occur;

4.7 Success Factors

A number of critical factors will contribute to the success of the malicious code analysis effort. Chief among them are: 1) the ability to interface and interact with community peers on a recurring basis; 2) the ability to stay abreast of the current state of the technology; 3) recognition by peers as a worthwhile and productive contributor to the overall community effort to analyze malicious code; and perhaps most importantly, 4) the establishment of trust relationships with other malicious code analysis efforts that will foster a mutual working environment conducive to the analytic process.

5 EINSTEIN³

5.1 Overview

The Einstein Program is a partnership between US-CERT and federal community to aid agencies in their ability to monitor and analyze network anomalies. Federal agencies will be required to participate in this program that allows the US-CERT to better understand the broader trends impacting the overall federal government in support of National Security Presidential Directive Thirty-Eight, Homeland Security Presidential Directives Five and Seven, and the National Strategy to Secure Cyberspace.

The Einstein Program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. By collecting information at the Internet gateway of participating federal government agencies, the US-CERT builds and enhances our nation's cyber-related situational awareness. Awareness will facilitate identifying and responding to cyber threats and attacks, and increases the resiliency of critical, electronically delivered government services.

The Program supports Federal agencies' efforts to protect their computer networks. System and network administrators within each agency are responsible for guarding access to sensitive information and computing infrastructure. During the past several years, network attacks and disruptions have become increasingly common and occur at rates that prevent government officials from managing risks effectively without a collective and collaborative information-sharing program. Both statutory provisions and the Office of Management and Budget require agencies to share incident and risk data with the US-CERT to accomplish these goals.

Most of the Federal government's Internet-based services are provided individually by each agency within its local jurisdictional boundaries, culture, and unique information system. However, proper management of cyber risks requires that the agencies work collaboratively on information security issues in order to foster situational awareness.

There are no established processes for automating information sharing of cyber vulnerabilities and incidents. Currently, information reporting from Federal agencies to the US-CERT occurs manually. As a consequence, the limited information exchange that does occur happens primarily after the fact, when multiple systems in the Federal infrastructure already may have been affected. Experience with recent cyber attacks has demonstrated that effective defenses require accelerated information-sharing, analysis, and enhanced response preparation.

Federal agency partners are core to the functionality of the US CERT Einstein program. Each federal agency administrator retains complete control of network data in strict accordance with federal laws and policies. Agencies gather and subsequently share security data directly with the US-CERT. In turn, the US-CERT prepares a strategic, cross-agency assessment, which is then shared back with all federal civilian agencies. In return for sharing anomaly and security data,

³ The name of the program is currently under review – all references are for internal Government use only.

federal civilian agencies are better positioned to protect their systems, save scarce resources, and provide essential services.

5.2 Phased Approach

The Einstein Program is a three-phase effort. The first phase assessed the issues and solutions; evaluated and tested candidate solutions; and the development of the program Privacy Impact Assessment. The first phase concluded at the end of FY2004.

The second phase consists of developing all necessary program documentation and deploying the candidate solution at 6-8 federal agencies. Additionally, this phase will develop a broader understanding of the operational procedures and concepts by which the participating federal agencies will interact with the US-CERT and address technical and policy integration issues. The second phase will conclude at the end of FY2005 and provide the concrete information necessary to select the best course of action for the third phase.

The third phase will address several operational implementation strategies to provide coverage for the remaining federal agencies. These approaches will be based upon the conclusions derived from phase two and will also allow for the addition of broader analysis tools.

Phase three will also give the US-CERT the opportunity to refine the operational processes and procedures to better serve federal government agencies and render a more accurate cross government perspective.

5.3 Technical Overview – Current Phase

The current phase is fielding the network flow analysis tool QRadar from Q1Labs to understand the Internet threats to the federal community.

Participating agencies will receive at no charge the Q1 Labs QRadar product; hardware on which to run this product; and technical support and training.

The collection systems will be deployed at the agency's Internet Access Point (IAP) monitoring traffic sent to and from the Internet. Due to varying data filtering policies across agencies, Einstein must be deployed in front of the agencies Internet facing router or firewall. From this vantage point, Einstein will passively create flows from a provided communication splitter device or spanning port. The generated flows will be stored in a database kept at the agency. This local storage will allow the agency's security analysts to use the suite of analysis tools provided to better understand their network.

The provided software will allow the agency to locally analyze network anomalies and behavior, as well as, simultaneously sharing summary and statistical information with the US-CERT.

The summary and statistical information will be provided to the US-CERT over the Internet through an encrypted connection. This shared information will have no packet payload information, and will consist only of aggregated network flow records and traffic characterizations. Furthermore, only traffic crossing the IAP will be observed. Hence, no internal agency traffic should be visible to Einstein.

From this data sharing with the participants, the US-CERT will maintain a collection of summary and statistical reports on which it will perform cross-agency analysis of network

FOR OFFICIAL USE ONLY

anomalies in near real-time. Analysis reports resulting from the cross-agency analysis will be communicated to all federal agency participants.

5.3 Operational Capabilities and Benefits

The Einstein Program provides an efficient and cost-effective way to comply with legal requirements and protect critical systems. In operating the Einstein Program, the US-CERT will significantly strengthen the security posture of the federal government through increased situational awareness. The US-CERT will provide both technical support and program management.

US-CERT analysis will provide agencies with a better understanding of their current security status as it relates to the overall government security status and the status of Internet security generally. In addition, agencies will be able to perform analyses that will help to increase the security and understanding of potential security problems on their networks. Einstein will help agencies identify baseline network traffic patterns, configuration problems, unauthorized network traffic, network backdoors, routing anomalies, and network scanning activities.

The following capabilities and benefits will be provided for network security engineers and administrators to help address common security weaknesses and promote the cyber security of government systems:

- **Worm Detection:** Sharing and collaborating on IT incidents, threat, and vulnerabilities produces a sophisticated picture of attacks across the Federal.gov domain. The US-CERT provides this information directly to network administrators for the benefit of department and agency systems protection.
- **Anomalous Activity – In- and out-bound:** Similarly, in culling out certain cross-agency indicia – such as known criminal behavior or traffic that is highly suggestive of criminal behavior – the capability offers directly to the department and agency administrators an easy to understand picture on priority emergencies and needs. In the absence of such information, administrators must continue to rely on insufficient information to leverage scarce resources and to protect their systems.
- **Configuration Management:** The US-CERT will be able to provide counsel on configuration management options. Configuration challenges are fast becoming one of the most difficult problems for agency administrators. The Einstein Program offers information and options – based on a collective and collaborative approach.
- **Trends Analysis:** The US-CERT uses the information collected and analyzed to generate a cross-governmental trends analysis. The analysis offers to departments and agencies an accurate and aggregate picture on the health of the Federal.gov domain. The information is offered in real-time, and may include an assessment of anomalous amounts of network traffic across the Federal.gov domain – or, in

FOR OFFICIAL USE ONLY

some cases, within a single agency. The data can also offer an aggregate comparison on the health of the Federal.gov domain as compared to the Internet or even portions of the national network.

Einstein will provide the US-CERT and Federal agencies with a capability to detect behavioral anomalies within their networks. By analyzing the data and detecting these anomalies, the ability to detect new exploits and attacks in cyberspace will be greatly increased. Enhancing the ability to act swiftly in today's rapidly changing electronic environment is essential to protect government systems.

The following are examples of the various analytic processes and products that the Einstein Program will produce to protect the participating Federal agencies:

- Determine the scope and impact of any specific worm across the Federal government and how it relates to the Internet community at large;
- Detect anomalous network behavior or activities against the Federal government and determine whether it's a focused attack or part of a larger Internet-related activity;
- Determine the level of impact and any damage associated with cyber attacks against the Federal government;
- Diagnose specific Federal agency Internet traffic problems as they relate to the much larger Internet backbone infrastructure;
- Pinpoint the apparent source responsible for any cyber-related attacks;
- Determine the cyber state of the Federal government in near real-time and its interaction with the global Internet community;
- Compile an overall situational awareness of trends and traffic patterns for all participating Federal agencies;
- Detect early warning and indications of emerging attacks and malicious reconnaissance activities and adverse impact on Federal government agencies; and
- Correlate system compromises within the Federal government.

5.4 Conclusion

One of the main goals of the Einstein Program is to improve the quality, quantity, and speed of sharing information. By participating in the Einstein Program, Federal agencies will benefit by raising the cyber situational awareness for their individual agency, contribute to their meeting statutory requirements concerning information security, and contribute to the overall effort to build the government cyber situational awareness.

FOR OFFICIAL USE ONLY

In addition, agency participation assists US-CERT in determining the best ways to help agencies protect themselves, and contributes to the ability of US-CERT to provide timely alert and warning information to government.

Federal agency participation is paramount to the overarching situational awareness capabilities the Einstein Program can offer and its collaborative benefits. The use of this automated analysis capability by the Federal government agencies represents one way that the US-CERT is leveraging current operational technology to significantly increase the overall situational awareness of our Nation's Cyberspace, as well as, the Internet community at large.

FOR OFFICIAL USE ONLY

- 30 -

APPENDIX A

A HSIN/US-CERT PORTAL

A.1 Overview

The HSIN/US-CERT Portal is more than an incident reporting mechanism it is an information dissemination mechanism to communicate relevant cyber information. Through a suite of tools such as secure messaging, forms, secure chat rooms, alerts and shared libraries US-CERT is able to push necessary information to a broad or targeted audience. For example, if the US-CERT Operation Center assigns a severity rating of 5 to a piece of cyber security information, using the alert function in the HSINS/US-CERT Portal would be appropriate because the alert tool would be the quickest way to push that critical information to a portal user.

To submit information securely, US-CERT has established the HSIN/US-CERT Portal, a secure, web-based collaborative system that allows members to communicate and collaborate on a real time, 24x7 basis about emerging cyber threats and vulnerabilities. Agencies can request a portal account by going to the HSIN/US-CERT Portal homepage (<https://gfirst.us-cert.gov>) and clicking on the “here” tab underneath the login field.

The portal contains four forums that portal members can use to collaborate on a real-time basis as necessary. The forums provide an opportunity for members to discuss suspicious activity, ask for advice, post news articles and discuss topics of interest with other members. Forums have the ability to be established for a specific audience or can be created so that access is granted for everyone. Both US-CERT Operations team and individual members of the portal have the ability to create a new thread, as they would like.

The forums are: 1) Emerging Threats Forum, 2) Malware Code Analysis Forum, 3) Incident Response Forum, and 4) Vulnerabilities Forum. Information is posted to each respective forum as soon as new information is made available.

A.1.1 Emerging Threat Forum

The Emerging Threat Form focuses on anomalies and events that users and the US-CERT Watch identify as possible threats. Discussion may include analysis of “spikes” on certain ports, the relevance of such anomalies, and probable causes. Sample threads include: “Odd Scans,” “X Worm,” “Port X Spike,” “New Variant,” etc. A thread can be started by either US-CERT or a member organization. To receive notification of a new thread, members can subscribe to a forum by clicking on the “subscribe” link in the portal.

A.1.2 Malware Code Analysis Forum

The Malware Code Analysis Forum focuses on the methods, tools, and other topics related to malware and the analysis of malicious code. This is an ideal place for malware experts to share information regarding new exploits in the wild such as payload, method of propagation, impact, breath of distribution, and speed of propagation.

A.1.3 Incident Response Forum

The Incident Response Forum focuses on response to cyber security events and how various incident response teams are handling them. Discussions in this forum may also include the

FOR OFFICIAL USE ONLY

practices, procedures, and metrics that different organizations have found effective. Unless specifically mentioned by a portal member, US-CERT does not disclose any information about any specific organization or government agency to protect individual's identities. Information provided will be in actionable, general terms.

A.1.4 Vulnerabilities Forum

The Vulnerabilities Forum focuses on recent vulnerabilities and various strategies for response and prevention. The discussion may include input about vulnerabilities' effect, impact, and lessons learned.

APPENDIX B

B CYBER FORENSICS TRAINING

B.1 Overview

There are many emerging technologies that incident response teams have to stay current with in order to conduct incident analysis to determine if a cyber event was a policy violation, possibly criminal, or malicious in nature such as a worm or new virus. This includes determining how the cyber event was executed.

In order to determine the nature of the incident a forensic effort must be undertaken at the host, network, or device level. These efforts are often tedious and require special tools, techniques, and time to conduct. Not all agencies have the required tools, forensic personnel, and ability to conduct forensic analysis. US-CERT will develop a training program partnering with CERT/CC and Law Enforcement to increase agency's forensic capabilities. This will increase the number of forensic subject matter experts and increase response times within agencies due to having trained personnel.

In FY06/07 US-CERT will further enhance this program by maintaining a list of forensic subject matter experts, including US-CERT personnel, and provide specialized equipment or forensic tools that agencies can leverage during the analysis of a cyber event impacting their organization.

B.2 Objectives

It is the intent of US-CERT to assist agencies with the following activities;

1. Forensic Education Program which will go over the following topics
 - a. Overview of Forensic tools, how to utilize them, and which ones are applicable for a particular device, host operating system, and used in conducting network forensics
 - b. Forensic techniques based on best practices from incident response teams & law enforcement examiners
 - c. Policy and Procedure development
 - d. Expert witness training
2. Forensic Policy & Procedural Development
 - a. Assist agencies in developing formal forensic policies and procedures for their parent organization by making available templates and best practices on cyber forensics through NIST & US-CERT

FOR OFFICIAL USE ONLY

B.3 Primary Benefits

1. US-CERT will develop and offer a training program in partnership with CERT/CC to increase agency capabilities by teaching cyber forensic techniques, forensic tools, and how to follow the digital forensic trail.

2. Agencies that need assistance can utilize trained subject matter experts or US-CERT personnel to help reduce forensic work load in order to wrap up cyber investigations that might involve policy violations, cyber incidents, and identification of malware.

3. US-CERT will acquire and provide loaner forensic equipment including a forensic laboratory in which agencies can have access to tools that they might not otherwise have access to due to fiscal constraints.

APPENDIX C

C CNDSP PROGRAM

C.1 Overview

US-CERT has the opportunity to effectively implement the National Strategy to Secure Cyberspace, increase partnerships with other agencies, and provide a more secure environment for the U.S. government. Significant progress in these areas can be accomplished by administering a Computer Network Defense Service Provider (CNDSP) Accreditation Program similar to what the Department of Defense has implemented.

This effort would be a cooperative, iterative, program between National Institute of Standards & Technology (NIST), Department of Homeland Security (DHS), Office of Management & Budget, Federal Incident Response Teams (GFIRST), and the DoD.

The first phase is to adapt the program from the Defense community to the Federal Agency's security requirements through a collaborative effort. Then US-CERT, in partnership with CERT/CC, will conduct a self assessment of US-CERT, develop an improvement plan, and implement the necessary changes. Once completed an independent organization will evaluate US-CERT to become an accrediting authority for conducting CNDSP reviews.

The next phase will be to evaluate Department Level Incident Response Teams after they have gone through a self assessment and made improvements according to the evaluation criteria of the CNDSP. Once they are evaluated by US-CERT they will become an accrediting authority for their Department and will then evaluate their Bureau Incident Response Capabilities.

This program will provide clear performance metrics, consistency across incident response teams, including all operational procedures and process are documented. In addition, it will provide the opportunity to ensure that contractor services are adequately secure and that a capable mechanism is in place to detect, report, and share information on vulnerabilities which were identified as common government wide security performance gap by OMB.

C.2 Objectives

It is the intent of US-CERT to assist agencies with the following activities;

1. Develop and implement a Computer Network Defense Service Provider (CNDSP) program for the government.
2. Test and adapt metrics for application to federal agencies through pilot program.
3. Refine scoring metrics based on results of the pilot program.
4. Develop a government wide implementation strategy.

FOR OFFICIAL USE ONLY

5. Perform scheduled evaluations of CNDSP capabilities in the government.
6. Provide process improvement plans and assistance to help federal government teams meet the government standard.
7. Improve and refine the program for federal government.

C.3 Primary Benefits

1. Improve the security posture of government information systems and networks by:
 - a. Standardizing incident response actions across the government.
 - b. Improving level of support provided by incident response providers.
 - c. Insuring the readiness of government incident response teams to handle cyber events in a consistent manner
2. Establish a baseline standard for capabilities that should exist within federal government incident response capabilities

Assist agencies with developing and implementation of process improvement plans in order to ensure that they meet the government standard baseline for CNDSP.

APPENDIX D**D GLOSSARY****C**

| | |
|---------|------------------------------------------------------|
| CERT | Computer Emergency Response Team |
| CERT/CC | Computer Emergency Response Team Coordination Center |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CM | Configuration Management |
| CNDSP | Computer Network Defense Service Provider |
| CONOPS | Concept of Operations |
| COTR | Contracting Officer Technical Representative |
| CSIRC | Computer Security Incident Response Center |
| CSIRT | Computer Security Incident Response Team |

D

| | |
|--------|-----------------------------------------------------------|
| DHS | Department of Homeland Security |
| DHS/IA | Department of Homeland Security Information Analysis |
| DHS/IP | Department of Homeland Security Infrastructure Protection |
| DNS | Domain Name Service |
| DoD | Department of Defense |
| DoS | Denial of Service |

F

| | |
|-------|---------------------------------------------|
| FIN | Federal Information Notice |
| FISMA | Federal Information Security Management Act |

G

| | |
|--------|------------------------------------------------------|
| GFIRST | Government Forum of Incident Response Security Teams |
|--------|------------------------------------------------------|

H

| | |
|------|---------------------------------------|
| HSIN | Homeland Security Information Network |
| HSOC | Homeland Security Operations Center |
| HSC | Homeland Security Council |

I

| | |
|------|----------------------------------------------------|
| IAIP | Information Analysis and Infrastructure Protection |
| IAP | Internet Access Point |
| IC | Intelligence Community |
| ICD | Infrastructure Coordination Division |
| IDS | Intrusion Detection System |

FOR OFFICIAL USE ONLY

| | |
|---------|----------------------------------------------------------------|
| IIMG | Interagency Incident Management Group |
| ISAC | Information Sharing and Analysis Center |
| ISP | Internet Service Provider |
| IT | Information Technology |
| IT-ISAC | Information Technology Information Sharing and Analysis Center |

J

| | |
|---------|--------------------------------------------|
| JTF-GNO | Joint Task Force Global Network Operations |
|---------|--------------------------------------------|

M

| | |
|---------|-----------------------------------------------------|
| MS-ISAC | Multi-State Information Sharing and Analysis Center |
|---------|-----------------------------------------------------|

N

| | |
|--------|----------------------------------------------------------|
| NAC | Nebraska Avenue Complex |
| NASCIO | National Association of State Chief Information Officers |
| NCRCG | National Cyber Response Coordination Group |
| NCS | National Communications System |
| NCSD | National Cyber Security Division |
| NICC | National Infrastructure Coordinating Center |
| NIPP | National Infrastructure Protection Plan |
| NIST | National Institute of Standards and Technology |
| NOC | Network Operations Center |
| NSC | National Security Council |

O

| | |
|-----|---------------------------------|
| OMB | Office of Management and Budget |
| OVP | Office of the Vice President |

P

| | |
|-----|-----------------------------|
| PGP | Pretty Good Privacy |
| PSD | Protective Service Division |

S

| | |
|-----|-------------------------------|
| SSC | Sector Coordinating Council |
| SOC | Security Operations Center |
| SOP | Standing Operating Procedures |
| SPO | Strategic Partnership Office |

T

| | |
|------|-------------------------------------------------------------------|
| TSA | Transportation Security Administration |
| TSOC | Transportation Security Administration Security Operations Center |

U

| | |
|---------|-------------------------------------------------|
| US | United States |
| US-CERT | United States Computer Emergency Readiness Team |

FOR OFFICIAL USE ONLY

Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructure

1. whether the agency is on track with respect to its improvement plansFor Federally controlled information systems and Federally controlled systems supporting critical infrastructure:

Identified goals have been reached for two out of eleven performance measures:

- The percentage of systems assigned a risk impact level is 92%. The FY06 goal was 80%.
- IGs at 18 out of 25 agencies have verified agency oversight of contractor systems. The FY06 goal was 18 agencies.

Improvements in performance have been achieved for two out of the nine remaining performance measures:

- Implementation of the Einstein tool
- Planning for the Information Systems Security Line of Business

Decreases in performance have been seen in the following two metrics:

- Testing of security controls
- Testing of contingency plans

Agencies have demonstrated mixed performance on the following metric:

- System certification and accreditation (the overall rate dropped slightly but the rate for high impact systems increased)

There has been no change in the following four metrics:

- IG verification of the plan of action and milestone process
- IG assessment of the certification and accreditation process
- Implementation of security configurations
- Government wide contracts for contractor security hardware, software and services

In accordance with OMB Instructions for Preparing the Federal Information Security Management Act Report, agencies will submit third quarter FY06 FISMA data on June 15. This data may reflect improvement in agency security performance.

For the Nation's Critical Infrastructure

DHS-NCSD is on track for the development of the IT Sector Specific Plan and the related components outlined on page 8 of the High Risk Plan.

2. major deliverables the agency has accomplished in the last six months

For Federally controlled information systems and Federally controlled systems supporting critical infrastructure:

- The percentage of high impact systems with a certification and accreditation has increased from 88% to 90%. The C&A goal for high impact systems is 95% by the end of FY06.
- The Einstein detection tool is undergoing certification and accreditation at one additional agency. Five installations have been completed to date. The FY06 goal is eight installations.
- On June 7th, OMB signed a designation letter making DHS the managing agency for the Information Systems Security Line of Business. DHS has initiated staffing for the program management office. Plans to create shared service centers for security training and FISMA reporting are proceeding.
- The following performance metrics remain unchanged.
 - IGs at 19 out of 25 agencies verify the effectiveness of the Plan of Action and Milestone process. The FY06 goal is 20 agencies with an effective Plan of Action and Milestone process.
 - IGs at 17 out of 25 agencies continue to rate certification and accreditation programs as "good" or "satisfactory". The FY06 goal is 20 agencies with a satisfactory or better process.
 - 22 agencies have an agency-wide security configuration policy. The goal is for 70% of all systems and 80% of high impact systems to implement security configurations.

- There has been no increase in the number of government wide contracts available for security hardware, software and services. The goal is three contracts by the end of FY06.

For the Nation's Critical Infrastructure

No deliverables on the High Risk Plan for the IT Sector Specific Plan were due in the last six months. However, DHS-NCSD is on a good trajectory to meet the Q1 and Q2 FY07 items. (As a reminder, our dates were revised based on the new dates for the NIPP. The IT Sector Specific Plan dates were pushed by 6 months since the NIPP release was also pushed by 6 months.) DHS-NCSD is actively engaged with IT Sector Coordinating Council and Government Coordinating Council to develop the IT Sector Specific Plan. The first annotated outline has been developed and is undergoing public and private sector review/comment. A jointly developed delivery schedule has also been created that DHS-NCSD is aggressively pursuing with public and private IT sector partners for delivery of the IT Sector Specific Plan and its components in December 2006 (Q1 FY07).

3. major promised deliverables the agency failed to accomplish in the last 4 months

For Federally controlled information systems and Federally controlled systems supporting critical infrastructure:

- Certification and accreditation
 - The overall percentage of systems with a certification and accreditation has dropped one percentage point to 84%. The goal is for 90% of all systems to be certified and accredited by the end of FY06.
- Contingency Plans
 - Testing of contingency plans has decreased from 61% to 58%. The goal is for 65% of all contingency plans to be tested by the end of FY06.
 - Testing of contingency plans for high impact systems stands at 63%. The goal is for 95% of contingency plans for high impact systems to be tested by the end of FY06.
- Testing of security controls
 - The percentage of agency systems with tested security controls has dropped from 72% to 67%. The goal for testing all systems is 85% by the end of FY06.
 - The percentage of high impact systems with tested security controls is 70%. The goal is 95% of high impact systems by the end of FY06.

For the Nation's Critical Infrastructure:

None

4. whether GAO has been adequately consulted on agency plans to address the area

For Federally controlled information systems and Federally controlled systems supporting critical infrastructure:

Yes, OMB coordinates with GAO on the status of agency security programs. OMB regularly meets with GAO to discuss the findings of GAO information security reviews. Each March OMB prepares an annual report to Congress on agency compliance with the Federal Information Security Management Act. GAO analyzes this data as well.

For the Nation's Critical Infrastructure

Through OMB, the GAO has been consulted and kept apprised of the status of the High Risk Plan action items.

5. any suggested intervention Clay or Robert could provide to improve progress in the area.

None at this time

Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures

OMB Contact: Kim Johnson (202-395-7232)

DHS Owner: Andy Purdy (703-235-5125)

DHS Contact: Andy Purdy (703-235-5125)

GAO Contacts: Joel Willemsen (202-512-6408)

Scope: Protecting federal computer systems and the systems that support critical infrastructures.

Overall: Develop a long-range plan to improve the effectiveness and efficiency of information security programs.

Short-Term: Within two years, for Federally controlled information systems and Federally controlled systems supporting critical infrastructures, OMB, DHS, NIST, and national security authorities will work with the departments and agencies to reduce risk through better planning for and more consistent implementation of security controls and improved performance measurement of agency security programs and processes.

For information systems supporting critical infrastructures beyond Federal control within two years, DHS will finalize and implement the National Infrastructure Protection Plan (NIPP) and the Information Technology Sector Specific Plan (IT SSP). These plans provide the risk management framework for reducing vulnerabilities, deterring threats, and minimizing consequences of attacks to critical infrastructure and key resources. The NIPP and IT SSP are discussed in more detail on page 6.

Focus areas for Federally controlled information systems and Federally controlled systems supporting critical infrastructures:

1. Increase compliance with the Federal Information Security Management Act (FISMA), HSPD-7, and guidance concerning agency continuity of operations and national security/emergency preparedness telecommunications through:
 - Integrating requirements of FISMA, HSPD-7, FEMA guidance and NCS Directives to simplify processes and promote consistent implementation across government,
 - Continue to define and prioritize Federally controlled information systems by risk levels,
 - Increase the number of IT systems meeting key FISMA performance measures, and
 - Improve the quality of agency FISMA processes through increased qualitative assessments by agency Inspectors General and other independent experts as appropriate.
2. Promote more cost effective implementation of key security controls through developing common security solutions.
 - Achieve greater efficiency and effectiveness through standardizing and sharing capabilities, skills, and processes across government, to the maximum extent practicable (i.e., implementing the Information Systems Security Line of Business)

Process for Federally controlled information systems and Federally controlled systems supporting critical infrastructures

1. OMB/DHS provide major initiatives and goals for each focus area.
2. OMB/DHS identify milestones for meeting goals for initiatives identified.
3. OMB/DHS indicate what metrics will be used to measure improved performance.
4. OMB/DHS concurrence on goals, milestones, and metrics.
5. Senior DHS leadership buy-in obtained.
6. Monitor progress with quarterly staff meetings and quarterly/semi-annual updates.
7. Quarterly and semi-annual reports will be prepared as applicable.

Responsible Organizations:

For Federally controlled information systems and Federally controlled systems supporting critical infrastructures -- the Office of Management and Budget through the Administrator, Office of E-Government and Information Technology and the Department of Homeland Security through the Assistant Secretary for Infrastructure Protection and Director of National Cyber Security Division are responsible for identifying the goals and overseeing the initiatives cited in this Plan, but effective execution largely depends on departments and agencies.

For information systems and systems supporting critical infrastructures beyond Federal control, the Department of Homeland Security through the Director, National Cyber Security Division is responsible for identifying the goals and overseeing the initiatives cited in this Plan, but effective execution is beyond Federal control depending on actions by private sector owners and operators.

Goals for Federally controlled information systems and Federally controlled systems supporting critical infrastructures:

The goals under this plan are to improve the protection of Federally controlled information systems and Federally controlled systems supporting critical infrastructures using the following measures and others to be developed later to:

- Determine immediate and root causes of current information security vulnerabilities and gaps,
- Provide leadership and direction for mitigating the risk from these vulnerabilities and gaps,
- Implement a set of risk-based, cost-effective controls and measures to adequately protect information and Federally controlled information systems, and
- Adapt to rapidly changing technologies and risk environments.

Metrics and Baselines 3rd Quarter FY05 Status 2nd Quarter FY06 Status

| Metric | Federal Departments and Agencies | Federal Departments and Agencies |
|-----------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|
| FISMA compliance- Certification and accreditation | 79% of systems certified and accredited | 84% of systems certified and accredited |
| FISMA compliance -- Certification and accreditation | IGs rate 15 agencies as having good or satisfactory processes | IGs rate 17 agencies as having good or satisfactory processes |

| | | |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| FISMA compliance-- Plan of action and milestone | IGs verify the process at 18 agencies to remediate IT security weaknesses | IGs verify the process at 19 agencies to remediate IT security weaknesses |
| FISMA compliance -- Incident handling | Sporadic/low levels of reporting by some agencies | Sporadic/low levels of reporting by some agencies |
| FISMA compliance -- Incident handling | Einstein incident detection tool installed by DHS/NCSD at 2 Departments and agencies | Einstein incident detection tool installed by DHS/NCSD at 5 Departments and agencies |
| FISMA compliance -- Categorization of systems by risk impact level | Baseline data from agencies not currently available. | 92% of systems assigned a risk impact level. |
| FISMA compliance -- Tested contingency plans | 57% of contingency plans tested on an annual basis | 58% of contingency plans tested on an annual basis. |
| FISMA compliance -- Tested security controls | 76% of systems have security controls tested on an annual basis | 67% of systems have security controls tested on an annual basis. |
| FISMA compliance -- Agency oversight of contractor systems | IGs verify that 16 agencies have used appropriate methods to ensure that contractor provided services are adequately secure | IGs verify that 18 agencies have used appropriate methods to ensure that contractor provided services are adequately secure. |
| IT systems installed and maintained in accordance with security configurations. | Baseline data will be available September 15, 2005 | 22 agencies have an agency wide security configuration policy. |
| Efficiency -- information systems security line of business | FY07 business case currently in development. OMB established steering group to govern implementation. | DHS designated managing agency for the line of business. Staffing for the program management office is underway. |
| Efficiency -- development of contracting vehicles for security hardware, software, and services | 1 contracting vehicle for security training (USA Learning) | 1 contracting vehicle for security training (USA Learning). |
| Efficiency -- Establishment of Centers of Excellence for IT security products and services | None currently established | None currently established. |

Metrics and Fiscal Year Targets for Federal information systems:

| Metric | FY2006 | FY2007 | FY2008 |
|---------------------------------------------------|----------------------------|-----------------------------|-----------------------------|
| FISMA compliance- percentage of systems certified | 90% | 90% | 95% |
| | (95% of high risk systems) | (100% of high risk systems) | (100% of high risk systems) |

| | | | |
|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------------|------------------------------------|
| and accredited | | | |
| FISMA compliance -- Agencies with good or higher certification and accreditation processes | 20 | 22 | 24 |
| FISMA compliance— agencies with verified processes to remediate IT security weaknesses (plans of action and milestones) | 20 | 22 | 24 |
| FISMA compliance -- Incident handling – agencies with automated intrusion detection tool (Einstein) | 8 | 16 | 24 |
| FISMA compliance -- Categorization of systems by risk impact level | 80% | 100% | 100% |
| FISMA compliance -- Tested contingency plans | 65% (95% of high risk systems) | 80% (100% of high risk systems) | 90% (100% of high risk systems) |
| FISMA compliance -- Tested security controls | 85% (95% of high risk systems) | 90% (100% of high risk systems) | 95% (100% of high risk systems) |
| FISMA compliance -- Agencies using appropriate methods to ensure contractor provided services are | 18 | 20 | 24 |

| | | | |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| adequately secure | | | |
| FISMA compliance -- IT systems installed and maintained in accordance with security configurations. | security configurations implemented for greater than 70% of the systems inventory (80% of high risk systems) | security configurations implemented for greater than 80% of the systems inventory (100% of high risk systems) | security configurations implemented for greater than 96% of the systems inventory (100% of high risk systems) |
| Efficiency – government wide contracts available for security hardware, software, and services | 3 government wide contracts available | 5 government wide contracts available | 7 government wide contracts available |
| Efficiency – Establishment of Centers of Excellence for IT security products and services | 0 (planning phase) | 3 | 6 |

Initiatives:

OMB's major initiatives and the focus areas to which they contribute are shown below.

| Initiative | FISMA compliance | Cost effective implementation |
|-------------------------------|------------------|-------------------------------|
| Security Line of Business | | X |
| A-11 Budget Process | | X |
| FISMA reporting | X | |
| President's Management Agenda | X | |

Methodology for Evaluation:

The initiative lead is responsible for the initial assessment of the validity of the data for each of the initiatives and for tracking progress of the initiative. OMB and DHS will monitor the validity of the data as part of initiative implementation and reporting metrics as defined. Additionally, as needed independent groups (such as Inspectors General, GAO, and other experts) will validate data during planned engagements.

Focus areas for Nation's Critical Infrastructures

Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection* issued by the President on December 17, 2003, mandated development of a National Infrastructure Protection Plan (NIPP) as the primary vehicle to guide implementation of the United States' policy for enhancing protection of the nation's critical infrastructure and key resources (CI/KR). The Department of Homeland Security (DHS) is charged with developing the NIPP, which is currently in draft form and under internal review by DHS.

The NIPP provides an integrated, comprehensive approach to addressing physical, cyber, and human threats and vulnerabilities to address the full range of risks to the Nation. The Plan is based upon a risk management framework that prioritizes CI/KR protection activities based on threats, vulnerabilities, and consequences. It provides a roadmap for identifying CI/KR assets, assessing vulnerabilities, prioritizing assets, and implementing protection measures in each infrastructure sector, including the Information Technology (IT) Sector.

The purpose of the Plan is to provide the process and mechanisms to prioritize protection across sectors, so that resources are applied where they offer the most benefit for reducing vulnerability, deterring threats, and minimizing consequences of attacks. The NIPP defines roles and responsibilities for carrying out these activities and involves the integrated, coordinated support of Federal departments and agencies; State, local, and tribal entities; and public and private sector assets owners and operators, and international entities.

When completed, the NIPP and its component Sector Specific Plans, including the IT Sector Plan, will serve as the foundations for addressing the challenges to securing the nation's critical information infrastructure as identified by GAO. Specifically, the NIPP and IT Sector Plan address the GAO-identified actions for policy and guidance, trusted relationships, analysis and warning, and information sharing incentives that are discussed below.

1. Policy and guidance:

- Develop a comprehensive and coordinated national plan to facilitate CIP that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets time frames for achieving objectives, and establishes performance measures.

2. Trusted relationships:

- develop productive relationships within the federal government and between the federal government and state and local governments and the private sector.

3. Analysis and Warning Capability:

- Improve the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, and useful warnings and other information concerning both cyber and physical threats to federal and nonfederal entities.

4. Information sharing incentives:

- Provide appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other CIP efforts.

In addition, the NIPP and IT Sector Plan will address several of the GAO findings contained in GAO-05-827T "Critical Infrastructure Protection: Challenges in Addressing Cybersecurity" dated July 20, 2005. The NIPP and IT Sector Plan will increase awareness about cyber security roles and capabilities, facilitate effective partnerships with stakeholders, and improve two-way information sharing with these stakeholders.

Process:

1. DHS provide major initiatives and goals for each of the four focus areas.
2. DHS to identify milestones for meeting goals for initiatives identified.
3. DHS indicate what metrics will be used to measure improved performance.
4. OMB/DHS concurrence on goals, milestones, and metrics.
5. Clay Johnson/Bob Stephan/Andy Purdy meeting to obtain senior DHS leadership buy-in
6. Monitor progress with monthly staff meetings and quarterly updates.
7. A day of briefings will be held in August 2005 with quarterly reports beginning in October 2005.

Responsible Organizations:

The DHS Office of Infrastructure Protection and National Cyber Security Division are responsible for identifying the goals and overseeing the initiatives cited in this Plan, but depend on the DHS Preparedness Directorate and other entities to implement the initiatives and measure their results.

Goals:

DHS's goals under this plan are to improve the protection of the nation's critical infrastructures using the following measures and others to be developed later. Initial metrics are framed around process or outputs in developing plans and completing milestones. As the National Infrastructure Protection Plan (NIPP) and IT Sector Specific Plan (SSP) mature, outcome metrics will be developed and used in place of the following process-oriented metrics.

Metrics and Baselines - FY 2006 (End of Year):

| Initiative | Milestone | Completion Date |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------|
| NIPP | | |
| Develop NIPP base plan to serve as guiding framework for securing critical infrastructures (Note: the draft NIPP addresses the four focus areas and provides initiatives and goals that are directly relevant.) | Finalized NIPP Base Plan | Q3 FY06 |
| Develop Core metrics and Sector Specific metrics for NIPP performance measurement in collaboration with partners | NIPP Metrics Identification | Q1 FY07 |
| Develop performance measurement levels associated with each metric in collaboration with partners | Performance Measurement Thresholds/Levels | Q1 FY07 |
| Develop data collection methods in collaboration with partners | Data Collection Methods/Tools | Q1 FY07 |
| Identify metrics best practices already in use by some Sector Specific Agencies(SSA) | Metrics Best practices | Q1 FY07 |
| Collect the necessary data to assess/measure performance of each SSA | Sector Assessments | Annually, once first baseline assessment is conducted |
| Assess all sectors together to develop national assessment of the "state of CIP" | National CI/KR Protection Annual Report | Annually |
| Develop updates to metrics on a regular basis | Performance Metrics Updates | Annually |
| | | |

| | | |
|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|---------|
| IT Sector Specific Plan (SSP) | | |
| Develop a framework and process for developing IT sector-specific metrics | IT Sector Metrics Framework | Q1 FY07 |
| Develop IT sector-specific metrics in collaboration with partners | IT Sector Metrics document | Q1 FY07 |
| Develop data collection and reporting processes and tools | Metrics procedures and protocols document | Q2 FY07 |
| Develop IT Sector vulnerability assessment methodology | Vulnerability Assessment Methodology | Q1 FY07 |
| Identify protective measures for nationally critical IT Sector assets to mitigate vulnerabilities | Protective Measures Guidance | Q1 FY07 |
| Update IT SSP as part of annual review process | Revised IT SSP | Q1 FY07 |
| Continue to provide cross-sector cyber security support to various SSAs and federal agencies in their CIP efforts | Review and comment on cyber components of other SSPs | Q1 FY07 |

Metrics and Fiscal Year Targets:

As DHS continues to finalize the NIPP and IT SSP, metrics and fiscal year targets are being developed. The processes and plans for developing these metrics under the NIPP and IT SSP are attached. Note that these are in pre-decisional, draft format and are currently undergoing internal DHS review.

Initiatives:

DHS's major initiatives and the focus areas to which they contribute are shown below.

| Initiative | Policy & Guidance | Trusted Relationships | Analysis & Warning Capabilities | Information Sharing Incentives |
|-------------------------------|-------------------|-----------------------|---------------------------------|--------------------------------|
| NIPP | X | X | X | X |
| IT Sector Specific Plan (SSP) | X | X | | X |

Methodology for Evaluation:

The initiative lead is responsible for the initial assessment of the validity of the data for each of the initiatives and for tracking progress of the initiative. DHS components will establish a methodology for monitoring the validity of data as part of initiative implementation and reporting metrics as defined. Additionally, as needed independent groups (such as contractors, DHS IG, and GAO) will validate data during planned engagements.

United States Government Accountability Office

GAO

Testimony before the Subcommittee on
Federal Financial Management, Government
Information, and International Security, Senate
Committee on Homeland Security and
Governmental Affairs

For Release on Delivery
Expected at 9:30 a.m. EDT
Friday, July 28, 2006

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

Statement of David A. Powner
Director, Information Technology Management Issues

Keith A. Rhodes, Chief Technologist
Director, Center for Technology and Engineering



GAO-06-863T

July 2006

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan



Highlights of GAO-06-863T, a testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Since the early 1990s, growth in the use of the Internet has revolutionized the way that our nation communicates and conducts business. While the Internet originated as a U.S. government-sponsored research project, the vast majority of its infrastructure is currently owned and operated by the private sector. Federal policy recognizes the need to prepare for debilitating Internet disruptions and tasks the Department of Homeland Security (DHS) with developing an integrated public/private plan for Internet recovery.

GAO was asked to summarize its report being released today—*Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006). This report (1) identifies examples of major disruptions to the Internet, (2) identifies the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluates DHS plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts.

What GAO Recommends

In its report, GAO suggests that Congress consider clarifying the legal framework guiding Internet recovery and makes recommendations to DHS to strengthen its ability to help recover from Internet disruptions. In written comments, DHS agreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-863T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Pownier at (202) 512-9286 or pownierd@gao.gov.

What GAO Found

A major disruption to the Internet could be caused by a physical incident (such as a natural disaster or an attack that affects key facilities), a cyber incident (such as a software malfunction or a malicious virus), or a combination of both physical and cyber incidents. Recent physical and cyber incidents, such as Hurricane Katrina, have caused localized or regional disruptions but have not caused a catastrophic Internet failure.

Federal laws and regulations that address critical infrastructure protection, disaster recovery, and the telecommunications infrastructure provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption. Specifically, key legislation on critical infrastructure protection does not address roles and responsibilities in the event of an Internet disruption. Other laws and regulations governing disaster response and emergency communications have never been used for Internet recovery.

DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but these efforts are not complete or comprehensive. Specifically, DHS has developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure are not complete. In addition, the department has started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, progress to date on these initiatives has been limited, and other initiatives lack time frames for completion. Also, the relationships among these initiatives are not evident. As a result, the government is not yet adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Key challenges to establishing a plan for recovering from Internet disruptions include (1) innate characteristics of the Internet that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until these challenges are addressed, DHS will have difficulty achieving results in its role as a focal point for helping the Internet to recover from a major disruption.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join today's hearing on reconstitution of critical networks such as the Internet. Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. Our country has come to rely on the Internet as a critical infrastructure supporting commerce, education, and communication. While the benefits of this technology have been enormous, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support.

Federal regulation establishes the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including recovery efforts for public and private critical infrastructure systems.¹ Additionally, federal policy recognizes the need to be prepared for the possibility of debilitating Internet disruptions and tasks DHS with developing an integrated public/private plan for Internet recovery.² Last July, we testified before you on DHS's responsibilities for cybersecurity-related critical infrastructure protection.³ In that testimony, we discussed the status of DHS's efforts and challenges faced by DHS in fulfilling its responsibilities. We reported that DHS had much work ahead of it. In a related report, we recommended that DHS prioritize cybersecurity-related responsibilities—including establishing recovery plans for key Internet functions.⁴

As requested, our testimony summarizes a report we released that (1) identifies examples of major disruptions to the Internet, (2) identifies the primary laws and regulations governing recovery of the Internet in the

¹Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (Dec. 17, 2003).

²The White House, *National Strategy to Secure Cyberspace* (Washington D.C.: February 2003).

³GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005).

⁴GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

event of a major disruption, (3) evaluates DHS's plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts.⁵ The report includes matters for congressional consideration and recommendations to DHS for improving Internet recovery efforts. In preparing for this testimony, we relied on our work supporting the accompanying report. That report contains a detailed overview of our scope and methodology. All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

A major disruption to the Internet could be caused by a physical incident (such as a natural disaster or an attack that affects facilities and other assets), by a cyber incident (such as a software malfunction or a malicious virus), or by a combination of both physical and cyber incidents. Recent physical and cyber incidents have caused localized or regional disruptions, highlighting the importance of recovery planning. For example, a 2002 root server attack highlighted the need to plan for increased server capacity at Internet exchange points in order to manage the high volumes of data traffic during an attack. However, recent incidents have also shown the Internet as a whole to be flexible and resilient. Even in severe circumstances, the Internet did not suffer a catastrophic failure. Nevertheless, it is possible that a complex attack or set of attacks could cause the Internet to fail. It is also possible that a series of attacks against the Internet could undermine users' trust and thereby reduce the Internet's utility.

Several federal laws and regulations provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption. Specifically, the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 provide guidance on protecting our nation's critical infrastructures. However, they do not specifically address roles and responsibilities in the event of an Internet disruption. The Defense Production Act and the Stafford Act provide authority to federal agencies to plan for and respond to incidents of national significance like disasters and terrorist attacks. However, the Defense Production Act has never been used for Internet recovery. In addition, the Stafford Act does not authorize

⁵GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006).

the provision of resources to for-profit companies such as those that own and operate core Internet components. The Communications Act of 1934 and National Communication System authorities govern the telecommunications infrastructure and help ensure communications during national emergencies, but they have never been used for Internet recovery either. Thus, it is not clear how effective these laws and regulations would be in assisting Internet recovery.

DHS has begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts are not yet comprehensive or complete. Specifically, DHS has developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure are not complete. In addition, DHS has started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, progress to date on these initiatives has been limited, and other initiatives lack timeframes for completion. Also, the relationships between these initiatives are not evident. As a result, the risk remains that the government is not yet adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Key challenges to establishing a plan for recovering from Internet disruption include (1) innate characteristics of the Internet (such as the diffuse control of the many networks that make up the Internet and the private-sector ownership of core components) that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to entities working to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until these challenges are addressed, DHS will have difficulty achieving results in its role as a focal point for helping to recover the Internet from a major disruption.

Given the importance of the Internet infrastructure to our nation's communications and commerce, we suggested in our accompanying report, that Congress consider clarifying the legal framework guiding

Internet recovery.⁶ We also made recommendations to the Secretary of Homeland Security to strengthen the department's ability to serve effectively as a focal point for helping to recover from Internet disruptions by establishing clear milestones for completing key plans, coordinating various Internet recovery-related activities, and addressing key challenges to Internet recovery planning. In written comments, DHS agreed with our recommendations and provided information on initial activities it was taking to implement them.

Background

The Internet is a vast network of interconnected networks that is used by governments, businesses, research institutions, and individuals around the world to communicate, engage in commerce, do research, educate, and entertain. From its origins in the 1960s as a research project sponsored by the U.S. government, the Internet has grown increasingly important to both American and foreign businesses and consumers, serving as the medium for hundreds of billions of dollars of commerce each year. The Internet has also become an extended information and communications infrastructure, supporting vital services such as power distribution, health care, law enforcement, and national defense. Today, private industry—including telecommunications companies, cable companies, and Internet service providers—owns and operates the vast majority of the Internet's infrastructure. In recent years, cyber attacks involving malicious software or hacking have been increasing in frequency and complexity. These attacks can come from a variety of actors, including criminal groups, hackers, and terrorists.

Federal regulation recognizes the need to protect critical infrastructures such as the Internet. It directs federal departments and agencies to identify and prioritize critical infrastructure sectors and key resources and to protect them from terrorist attack. Furthermore, it recognizes that since a large portion of these critical infrastructures is owned and operated by the private sector, a public/private partnership is crucial for the successful protection of these critical infrastructures. Federal policy also recognizes the need to be prepared for the possibility of debilitating disruptions in cyberspace and, because the vast majority of the Internet infrastructure is owned and operated by the private sector, tasks DHS with developing an integrated public/private plan for Internet recovery. In its plan for protecting critical infrastructures, DHS recognizes that the Internet is a

⁶GAO-06-672.

key resource composed of assets within both the information technology and the telecommunications sectors.⁷ It notes that the Internet is used by all critical infrastructure sectors to varying degrees and provides information and communications to meet the needs of businesses and government.

In the event of a major Internet disruption, multiple organizations could help recover Internet service. These organizations include private industry, collaborative groups, and government organizations. Private industry is central to Internet recovery because private companies own the vast majority of the Internet's infrastructure and often have response plans. Collaborative groups—including working groups and industry councils—provide information-sharing mechanisms to allow private organizations to restore services. In addition, government initiatives could facilitate response to major Internet disruptions.

Federal policies and plans⁸ assign DHS lead responsibility for facilitating a public/private response to and recovery from major Internet disruptions. Within DHS, responsibilities reside in two divisions within the Preparedness Directorate: the National Cyber Security Division (NCSD) and the National Communications System (NCS). NCSD operates the U.S. Computer Emergency Readiness Team (US-CERT), which coordinates defense against and response to cyber attacks. The other division, NCS, provides programs and services that assure the resilience of the telecommunications infrastructure in times of crisis. Additionally, the Federal Communications Commission can support Internet recovery by coordinating resources for restoring the basic communications infrastructures over which Internet services run. For example, after Hurricane Katrina, the commission granted temporary authority for private companies to set up wireless Internet communications supporting various relief groups; federal, state, and local government agencies; businesses; and victims in the disaster areas.

Prior evaluations of DHS's cybersecurity responsibilities have highlighted issues and challenges facing the department. In May 2005, we issued a

⁷DHS, *The National Infrastructure Protection Plan*.

⁸These include the *National Strategy to Secure Cyberspace*, the interim *National Infrastructure Protection Plan*, the Cyber Incident Annex to the *National Response Plan*, and Homeland Security Presidential Directive 7.

report on DHS's efforts to fulfill its cybersecurity responsibilities.⁹ We noted that while DHS had initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 key cybersecurity responsibilities noted in federal law and policy. We also reported that DHS faced a number of challenges that have impeded its ability to fulfill its cyber responsibilities. These challenges included achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness of cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with stakeholders, and demonstrating the value that DHS can provide. In this report, we also made recommendations to improve DHS's ability to fulfill its mission as an effective focal point for cybersecurity, including recovery plans for key Internet functions. DHS agreed that strengthening cybersecurity is central to protecting the nation's critical infrastructures and that much remained to be done, but it has not yet addressed our recommendations.

Although Cyber and Physical Incidents Have Caused Disruptions, the Internet Has Not Yet Suffered a Catastrophic Failure

The Internet's infrastructure is vulnerable to disruptions in service due to terrorist and other malicious attacks, natural disasters, accidents, technological problems, or a combination of the above. Disruptions to Internet service can be caused by cyber and physical incidents—both intentional and unintentional. Recent physical and cyber incidents have caused localized or regional disruptions, highlighting the importance of recovery planning. However, these incidents have also shown the Internet as a whole to be flexible and resilient. Even in severe circumstances, the Internet has not yet suffered a catastrophic failure.

To date, cyber attacks have caused various degrees of damage. For example, in 2001, the Code Red worm used a denial-of-service attack to affect millions of computer users by shutting down Web sites, slowing Internet service, and disrupting business and government operations. In 2003, the Slammer worm caused network outages, canceled airline flights, and automated teller machine failures. Slammer resulted in temporary loss of Internet access to some users, and cost estimates on the impact of the worm range from \$1.05 billion to \$1.25 billion. The federal government coordinated with security companies and Internet service providers and released an advisory recommending that federal departments and agencies patch and block access to the affected channel. However, because the

⁹GAO-05-434.

worm had propagated so quickly, most of these activities occurred after it had stopped spreading.

In 2002, a coordinated denial-of-service attack was launched against all of the root servers in the Domain Name System. At least nine of the thirteen root servers experienced degradation of service. However, average end users hardly noticed the attack. The attack became visible only as a result of various Internet health-monitoring projects. The response to the attacks was handled by the server operators and their service providers. The attack pointed to a need for increased capacity for servers at Internet exchange points to enable them to manage the high volumes of data traffic during an attack. If a massive disruptive attack on the domain name server system were successful, it could take several days to recover from. According to experts familiar with the attack, the government did not have a role in recovering from it.

Like cyber incidents, physical incidents could affect various aspects of the Internet infrastructure, including underground or undersea cables and facilities that house telecommunications equipment, Internet exchange points, or Internet service providers. For example, on July 18, 2001, a 60-car freight train derailed in a Baltimore tunnel, causing a fire that interrupted Internet and data services between Washington and New York. The tunnel housed fiber-optic cables serving seven of the biggest U.S. Internet service providers. The fire burned and severed fiber optic cables, causing backbone slowdowns for at least three major Internet service providers. Efforts to recover Internet service were handled by the affected Internet service providers; however, local and federal officials responded to the immediate physical issues of extinguishing the fire and maintaining safety in the surrounding area, and they worked with telecommunications companies to reroute affected cables.

In addition, Hurricane Katrina caused substantial destruction of the communications infrastructure in Louisiana, Mississippi, and Alabama, but it had minimal affect on the overall functioning of the Internet outside of the immediate area. According to an Internet monitoring service provider, while there was a loss of routing around the affected area, there was no significant impact on global Internet routing. According to the Federal Communications Commission, the storm caused outages for over 3 million telephone customers, 38 emergency 9-1-1 call centers, hundreds of thousands of cable customers, and over 1,000 cellular sites. However, a substantial number of the networks that experienced service disruptions recovered relatively quickly.

Federal officials stated that the government took steps to respond to the hurricane, such as increasing analysis and watch services in the affected area, coordinating with communications companies to move personnel to safety, working with fuel and equipment providers, and rerouting communications traffic away from affected areas. However, private-sector representatives stated that requests for assistance, such as food, water, fuel, and secure access to facilities were denied for legal reasons; the government made time-consuming and duplicative requests for information; and certain government actions impeded recovery efforts.

Since its inception, the Internet has experienced disruptions of varying scale—including fast-spreading worms, denial-of-service attacks, and physical destruction of key infrastructure components—but the Internet has yet to experience a catastrophic failure. However, it is possible that a complex attack or set of attacks could cause the Internet to fail. It is also possible that a series of attacks against the Internet could undermine users' trust and thereby reduce the Internet's utility.

Existing Laws and Regulations Apply to the Internet, but Numerous Uncertainties Exist in Using Them for Internet Recovery

Several federal laws and regulations provide broad guidance that applies to the Internet infrastructure, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption because some do not specifically address Internet recovery and others have seldom been used. Pertinent laws and regulations address critical infrastructure protection, federal disaster response, and the telecommunications infrastructure.

Specifically, the Homeland Security Act of 2002¹⁰ and Homeland Security Presidential Directive 7¹¹ establish critical infrastructure protection as a national goal and describe a strategy for cooperative efforts by the government and the private sector to protect the physical and cyber-based systems that are essential to the operations of the economy and the government. These authorities apply to the Internet because it is a core communications infrastructure supporting the information technology and telecommunications sectors. However, this law and regulation do not specifically address roles and responsibilities in the event of an Internet disruption.

¹⁰The Homeland Security Act of 2002, Pub. L. No. 107-296 (Nov. 25, 2002).

¹¹Homeland Security Presidential Directive 7 (Dec. 17, 2003).

Regarding federal disaster response, the Defense Production Act¹² and the Stafford Act¹³ provide authority to federal agencies to plan for and respond to incidents of national significance like disasters and terrorist attacks. Specifically, the Defense Production Act authorizes the President to ensure the timely availability of products, materials, and services needed to meet the requirements of a national emergency. It is applicable to critical infrastructure protection and restoration but has never been used for Internet recovery. The Stafford Act authorizes federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency. However, the act does not authorize assistance to for-profit companies—such as those that own and operate core Internet components.

Other legislation and regulations, including the Communications Act of 1934¹⁴ and the NCS authorities,¹⁵ govern the telecommunications infrastructure and help to ensure communications during national emergencies. For example, the NCS authorities establish guidance for operationally coordinating with industry to protect and restore key national security and emergency preparedness communications services. These authorities grant the President certain emergency powers regarding telecommunications, including the authority to require any carrier subject to the Communications Act of 1934 to grant preference or priority to essential communications.¹⁶ The President may also, in the event of war or national emergency, suspend regulations governing wire and radio transmissions and authorize the use or control of any such facility or station and its apparatus and equipment by any department of the government. Although these authorities remain in force in the Code of Federal Regulations, they have been seldom used—and never for Internet recovery. Thus it is not clear how effective they would be if used for this purpose.

¹² Act of September 8, 1950, c. 932, 64 Stat. 798, as amended; codified at 50 U.S.C. App. Section 2061 *et seq.*

¹³ Pub. L. No. 93-288, 88 Stat. 143 (1974).

¹⁴ Communications Act of 1934 (June 19, 1934), ch. 652, 48 Stat. 1064.

¹⁵ Executive Order 12472 (Apr. 3, 1984), as amended by Executive Order 13286 (Feb. 28, 2003).

¹⁶ Executive Order 12472 § 2; Communications Act of 1934, § 706, 47 U.S.C. § 606.

In commenting on the statutory authority for Internet reconstitution following a disruption, DHS agreed that this authority is lacking and noted that the government's roles and authorities related to assisting in Internet reconstitution following a disruption are not fully defined.

DHS Initiatives Supporting Internet Recovery Planning Are under Way, but Much Remains to Be Done and the Relationship Between Initiatives Is Not Evident

DHS has begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts are not complete or comprehensive. Specifically, DHS has developed high-level plans for infrastructure protection and national disaster response, but the components of these plans that address the Internet infrastructure are not complete. In addition, DHS has started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. While these activities are promising, some initiatives are not complete, others lack time lines and priorities, and still others lack effective mechanisms for incorporating lessons learned. In addition, the relationship between these initiatives is not evident. As a result, the nation is not prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

High-Level Response and Protection Plans

DHS has two key documents that guide its infrastructure protection and recovery efforts, but components of these plans dealing with Internet recovery are not complete. The National Response Plan is DHS's overarching framework for responding to domestic incidents. It contains two components that address issues related to telecommunications and the Internet, Emergency Support Function 2 and the Cyber Incident Annex. These components, however, are not complete; Emergency Support Function 2 does not directly address Internet recovery, and the annex does not reflect the National Cyber Response Coordination Group's current operating procedures. The other key document, the *National Infrastructure Protection Plan*, consists of both a base plan and sector-specific plans. The base plan, which was recently released, describes the importance of cybersecurity and networks such as the Internet to critical infrastructure protection and includes an appendix that provides information on cybersecurity responsibilities. The appendix restates DHS's responsibility to develop plans to recover Internet functions. However, the base plan is at a high level and the sector-specific plans that would address the Internet in more detail are not scheduled for release until December 2006.

Several representatives of private-sector firms supporting the Internet infrastructure expressed concerns about both plans, noting that they would be difficult to execute in times of crisis. Other representatives were uneasy about the government developing recovery plans, because they were not confident of the government's ability to successfully execute the plans. DHS officials acknowledged that it will be important to obtain input from private-sector organizations as they refine these plans and initiate more detailed public/private planning.

Both the *National Response Plan* and *National Infrastructure Protection Plan* are designed to be supplemented by more specific plans and activities. DHS has numerous initiatives under way to better define its ability to assist in responding to major Internet disruptions. While these activities are promising, some initiatives are incomplete, others lack time lines and priorities, and still others lack an effective mechanism for incorporating lessons learned.

**National Communications
System Reorganization**

DHS plans to revise the role and mission of the National Communications System (NCS) to reflect the convergence of voice and data communications, but this effort is not yet complete. A presidential advisory committee on telecommunications¹⁷ established two task forces that recommended changes to NCS's role, mission, and functions to reflect this convergence, but DHS has not yet developed plans to address these recommendations.

**National Cyber Response
Coordination Group**

As a primary entity responsible for coordinating governmentwide responses to cyber incidents—such as major Internet disruptions—DHS's National Cyber Response Coordination Group is working to define its roles and responsibilities, but much remains to be done. DHS officials acknowledge that the trigger to activate this group is imprecise and will need to be clarified. Because key activities to define roles, responsibilities, capabilities, and the appropriate triggers for government involvement are still under way, the group is at risk of not being able to act quickly and definitively during a major Internet disruption.

¹⁷The National Security Telecommunications Advisory Committee advises the President on issues and problems related to implementing national security and emergency preparedness telecommunications policy.

Internet Disruption Working Group

Since most of the Internet is owned and operated by the private sector, NCSD and NCS established the Internet Disruption Working Group to work with the private sector to establish priorities and develop action plans to prevent major disruptions of the Internet and to identify recovery measures in the event of a major disruption. According to DHS officials who organized the group, it held its first forum, in November 2005, to begin to identify real versus perceived threats to the Internet, refine the definition of an Internet disruption, determine the scope of a planned analysis of disruptions, and identify near-term protective measures. DHS officials stated that they had identified a number of potential future plans; however, agency officials have not yet finalized plans, resources, or milestones for these efforts.

North American Incident Response Group

US-CERT officials formed the North American Incident Response Group, which includes both public and private-sector network operators that would be the first to recognize and respond to cyber disruptions. In September 2005, US-CERT officials conducted regional workshops with group members to share information on structure, programs, and incident response and to seek ways for the government and industry to work together operationally. While the outreach efforts of the North American Incident Response Group are promising, DHS has only just begun developing plans and activities to address the concerns of private-sector stakeholders.

Exercises

Over the last few years, DHS has conducted several broad inter-governmental exercises to test regional responses to significant incidents that could affect the critical infrastructure. More recently, in February 2006, DHS conducted an exercise called Cyber Storm, which was focused primarily on testing responses to a cyber-related incident of national significance. Exercises that include Internet disruptions can help to identify issues and interdependencies that need to be addressed. However, DHS has not yet identified planned activities, milestones, or which group should be responsible for incorporating lessons learned from the regional and Cyber Storm exercises into its plans and initiatives.

While DHS has various initiatives under way, the relationships and interdependencies between these various efforts are not evident. For example, the National Cyber Response Coordination Group, the Internet Disruption Working Group, and the North American Incident Response

Group are all meeting to discuss ways to address Internet recovery, but the interdependencies between the groups have not been clearly established. Without a thorough understanding of the interrelationships between its various initiatives, DHS risks pursuing redundant efforts and missing opportunities to build on related efforts.

After our report was issued, a private-sector organization released a report that examined the nation's preparedness for a major Internet disruption.¹⁸ The report stated that our nation is unprepared to reconstitute the Internet after a massive disruption. The report supported our findings that significant gaps exist in government response plans and that the responsibilities of the multiple organizations that would play a role in recovery are unclear. The report also made recommendations to complete and revise response plans such as the Cyber Incident Annex of the *National Response Plan*; better define recovery roles and responsibilities; and establish more effective oversight and strategic direction for Internet reconstitution.

Multiple Challenges Exist to Planning for Recovery from Internet Disruptions

Although DHS has various initiatives under way to improve Internet recovery planning, it faces key challenges in developing a public/private plan for Internet recovery, including (1) innate characteristics of the Internet that make planning for and responding to a disruption difficult, (2) lack of consensus on DHS's role and on when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to restore Internet service, (4) reluctance of the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until it addresses these challenges, DHS will have difficulty achieving results in its role as focal point for recovering the Internet from a major disruption.

First, the Internet's diffuse structure, vulnerabilities in its basic protocols, and the lack of agreed-upon performance measures make planning for and responding to a disruption more difficult. The components of the Internet are not all governed by the same organization. In addition, the Internet is international. According to private-sector estimates, only about 20 percent of Internet users are in the United States. Also, there are no well-accepted standards for measuring and monitoring the Internet infrastructure's

¹⁸Business Roundtable, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness* (Washington D.C.: June 2006).

availability and performance. Instead, individuals and organizations rate the Internet's performance according to their own priorities.

Second, there is no consensus about the role DHS should play in responding to a major Internet disruption or about the appropriate trigger for its involvement. The lack of clear legislative authority for Internet recovery efforts complicates the definition of this role. DHS officials acknowledged that their role in recovering from an Internet disruption needs further clarification because private industry owns and operates the vast majority of the Internet.

The trigger for the National Response Plan, which is DHS's overall framework for incident response, is poorly defined and has been found by both us and the White House to need revision.¹⁹ Since private-sector participation in DHS planning activities for Internet disruption is voluntary, agreement on the appropriate trigger for government involvement and the role of government in resolving an Internet disruption is essential to any plan's success.

Private-sector officials representing telecommunication backbone providers and Internet service providers were also unclear about the types of assistance DHS could provide in responding to an incident and about the value of such assistance. There was no consensus on this issue. Many private-sector officials stated that the government did not have a direct recovery role, while others identified a variety of potential roles, including

- providing information on specific threats;
- providing security and disaster relief support during a crisis;
- funding backup communication infrastructures;
- driving improved Internet security through requirements for the government's own procurement;
- serving as a focal point with state and local governments to establish standard credentials to allow Internet and telecommunications companies

¹⁹See GAO, *Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery*, GAO-06-442T (Washington, D.C.: Mar. 8, 2006), and the White House, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington, D.C., February 2006).

access to areas that have been restricted or closed in a crisis;

- providing logistical assistance, such as fuel, power, and security, to Internet infrastructure operators;
- focusing on smaller-scale exercises targeted at specific Internet disruption issues;
- limiting the initial focus for Internet recovery planning to key national security and emergency preparedness functions, such as public health and safety; and
- establishing a system for prioritizing the recovery of Internet service, similar to the existing Telecommunications Service Priority Program.

A third challenge to planning for recovery is that there are key legal issues affecting DHS's ability to provide assistance to help restore Internet service. As noted earlier, key legislation and regulations guiding critical infrastructure protection, disaster recovery, and the telecommunications infrastructure do not provide specific authorities for Internet recovery. As a result, there is no clear legislative guidance on which organization would be responsible in the case of a major Internet disruption. In addition, the Stafford Act, which authorizes the government to provide federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency, does not authorize assistance to for-profit corporations. Several representatives of telecommunications companies reported that they had requested federal assistance from DHS during Hurricane Katrina. Specifically, they requested food, water, and security for the teams they were sending in to restore the communications infrastructure and fuel to power their generators. DHS responded that it could not fulfill these requests, noting that the Stafford Act did not extend to for-profit companies.

A fourth challenge is that a large percentage of the nation's critical infrastructure—including the Internet—is owned and operated by the private sector, meaning that public/private partnerships are crucial for successful critical infrastructure protection. Although certain policies direct DHS to work with the private sector to ensure infrastructure protection, DHS does not have the authority to direct Internet owners and operators in their recovery efforts. Instead, it must rely on the private sector to share information on incidents, disruptions, and recovery efforts. Many private-sector representatives questioned the value of providing information to DHS regarding planning for and recovery from Internet

disruption. In addition, DHS has identified provisions of the Federal Advisory Committee Act²⁰ as having a “chilling effect” on cooperation with the private sector. The uncertainties regarding the value and risks of cooperation with the government limit incentives for the private sector to cooperate in Internet recovery-planning efforts.

Finally, DHS has lacked permanent leadership while developing its preliminary plans for Internet recovery and reconstitution. In addition, the organizations with roles in Internet recovery (NCS and NCSD) have overlapping responsibilities and may be reorganized once DHS selects permanent leadership. As a result, it is difficult for DHS to develop a clear set of organizational priorities and to coordinate between the various activities necessary for Internet recovery planning. In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department.²¹ These officials included the NCSD Director, the Deputy Director responsible for Outreach and Awareness, the Director of the US-CERT Control Systems Security Center, the Under Secretary for the Information Analysis and Infrastructure Protection Directorate and the Assistant Secretary responsible for the Information Protection Office. Additionally, DHS officials acknowledge that the current organizational structure has overlapping responsibilities for planning for and recovering from a major Internet disruption.

In a July 2005 departmental reorganization, NCS and NCSD were placed in the Preparedness Directorate. NCS’s and NCSD’s responsibilities were to be placed under a new Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. However, almost a year later, this position remains vacant. While DHS stated that the lack of a permanent assistant secretary has not hampered its efforts in protecting critical infrastructure, several private-sector representatives stated that DHS’s lack of leadership in this area has limited progress. Specifically, these representatives stated that filling key leadership positions would enhance DHS’s visibility to the Internet industry and potentially improve its reputation.

²⁰Pub. L. No. 92-463, 86 Stat. 770 (1972) codified at 5 U.S.C. app. 2.

²¹GAO-05-434.

**Implementation of
GAO
Recommendations
Should Improve DHS
Internet Recovery
Planning Efforts**

Given the importance of the Internet infrastructure to our nation's communication and commerce, in our accompanying report we suggested matters for congressional consideration and made recommendations to DHS regarding improving efforts in planning for Internet recovery.²² Specifically, we suggested that Congress consider clarifying the legal framework that guides roles and responsibilities for Internet recovery in the event of a major disruption. This effort could include providing specific authorities for Internet recovery as well as examining potential roles for the federal government, such as providing access to disaster areas, prioritizing selected entities for service recovery, and using federal contracting mechanisms to encourage more secure technologies. This effort also could include examining the Stafford Act to determine whether there would be benefits in establishing specific authority for the government to provide for-profit companies—such as those that own or operate critical communications infrastructures—with limited assistance during a crisis.

Additionally, to improve DHS's ability to facilitate public/private efforts to recover the Internet in case of a major disruption, we recommended that the Secretary of the Department of Homeland Security implement the following nine actions:

- Establish dates for revising the National Response Plan—including efforts to update key components that are relevant to the Internet.
- Use the planned revisions to the National Response Plan and the National Infrastructure Protection Plan as a basis to draft public/private plans for Internet recovery and obtain input from key Internet infrastructure companies.
- Review the NCS and NCSD organizational structures and roles in light of the convergence of voice and data communications.
- Identify the relationships and interdependencies among the various Internet recovery-related activities currently under way in NCS and NCSD, including initiatives by US-CERT, the National Cyber Response Coordination Group, the Internet Disruption Working Group, the North American Incident Response Group, and the groups responsible for developing and implementing cyber recovery exercises.

²²GAO-06-672.

-
- Establish time lines and priorities for key efforts identified by the Internet Disruption Working Group.
 - Identify ways to incorporate lessons learned from actual incidents and during cyber exercises into recovery plans and procedures.
 - Work with private-sector stakeholders representing the Internet infrastructure to address challenges to effective Internet recovery by
 - further defining needed government functions in responding to a major Internet disruption (this effort should include a careful consideration of the potential government functions identified by the private sector earlier in this testimony),
 - defining a trigger for government involvement in responding to such a disruption, and
 - documenting assumptions and developing approaches to deal with key challenges that are not within the government's control.

In written comments, DHS agreed with our recommendations and stated that it recognizes the importance of the Internet for information infrastructures. DHS also provided information about initial actions it is taking to implement our recommendations.

In summary, as a critical information infrastructure supporting our nation's commerce and communications, the Internet is subject to disruption—from both intentional and unintentional incidents. While major incidents to date have had regional or local impacts, the Internet has not yet suffered a catastrophic failure. Should such a failure occur, however, existing legislation and regulations do not specifically address roles and responsibilities for Internet recovery.

As the focal point for ensuring the security of cyberspace, DHS has initiated efforts to refine high-level disaster recovery plans; however, pertinent Internet components of these plans are not complete. While DHS has also undertaken several initiatives to improve Internet recovery planning, much remains to be done. Specifically, some initiatives lack clear timelines, lessons learned are not consistently being incorporated in recovery plans, and the relationships between the various initiatives are not clear.

DHS faces numerous challenges in developing integrated public/private recovery plans—not the least of which is the fact that the government does not own or operate much of the Internet. In addition, there is no consensus among public and private stakeholders about the appropriate role of DHS and when it should get involved; legal issues limit the actions the government can take; the private sector is reluctant to share information on Internet performance with the government; and DHS is undergoing important organizational and leadership changes. As a result, the exact role of the government in helping to recover the Internet infrastructure following a major disruption remains unclear.

To improve DHS's ability to facilitate public/private efforts to recover the Internet in case of a major disruption, our accompanying report suggested that Congress consider clarifying the legal framework guiding Internet recovery. We also made recommendations to DHS to establish clear milestones for completing key plans, coordinate various Internet recovery-related activities, and address key challenges to Internet recovery planning. Effectively implementing these recommendations could greatly enhance our nation's ability to recover from a major Internet disruption.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you have any questions on matters discussed in this testimony, please contact us at (202) 512-9286 and at (202) 512-6412 or by e-mail at pownerd@gao.gov and rhodesk@gao.gov. Other key contributors to this testimony include Don R. Adams, Naba Barkakati, Scott Borre, Neil Doherty, Vijay D'Souza, Joshua A. Hammerstein, Bert Japikse, Joanne Landesman, Frank Maguire, Teresa M. Neven, and Colleen M. Phillips.

Testimony of
Thomas E. Noonan
President and Chief Executive Officer
Internet Security Systems (ISS)

before the
Subcommittee on Federal Financial Management,
Government Information, and International Security
of the
Senate Committee on Homeland Security and
Governmental Affairs

Hearing on
“Cyber Security: Recovery and Reconstitution of Critical Networks”
July 28, 2006

* * *

Overview

Mr. Chairman, Mr. Ranking Member, distinguished members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Tom Noonan and I am President and Chief Executive Officer of Internet Security Systems (ISS).

ISS is the world’s leading provider of preemptive cyber security technologies for large-scale enterprises. Headquartered in Atlanta, Georgia, ISS employs thirteen hundred professionals with 35 offices in 20 countries worldwide. We operate five cyber Security Operations Centers spread across the globe – two in the United States, one in Tokyo, Australia, and Brussels – that scour the Internet for potential cyber threats 24 hours a day, 365 days a year and provide managed, preemptive protection for many of our customers. If it is on the Internet, ISS knows about it. ISS’ commitment to our government and private sector customers is to utilize our security intelligence, technology and expertise to preempt the strikes that could cripple critical networks and stay ahead of the threat.

As the representative of the security technology industry on this morning’s panel, I want to stress three important messages about our nation’s cyber security landscape:

- First, threats to our critical infrastructure are absolutely real and, without a doubt, growing. The question is not if, but when. The explosive growth of new Internet technologies, from wireless access to Voice over Internet telephony, has engendered threats that are far outpacing the security responses of private and governmental users.

- Second, the intelligence, protocols and technologies necessary to protect against emerging cyber threats are, by and large, robust and widely available. We *have* the tools at our disposal today to safeguard our critical infrastructure.
- And finally, despite our knowledge of these threats and our overall ability to protect ourselves, we as a nation are not doing nearly enough to *preempt* the types of attacks that could debilitate our critical networked infrastructure. Leadership is desperately needed at the Federal level -- not to *replicate* existing private sector efforts, but rather, to extend the impact of those efforts particularly by encouraging the private sector to collectively increase its cooperation. This means:
 1. Appointing an Assistant Secretary of Homeland Security for Cyber Security and Telecommunications who will help secure the Federal government's own networks as well as those of the broader economy;
 2. Clearly delineating and hardening the roles and responsibilities of the many public-private entities working today to secure cyberspace;
 3. Ensuring that the Federal Government makes full use of existing industry resources to gather and analyze data on cyber security threats;
 4. Creating a national plan to restore connectivity on a prioritized basis in the event of a large-scale cyber attack against our critical infrastructure; and
 5. Providing sustained Federal funding and active Congressional oversight to ensure that the Department of Homeland Security is getting the job done.

Cyber threats are serious, and they are growing in sophistication.

First, the bad news:

Cyber threats to our nation's critical infrastructure are not the stuff of hysteria or even hyperbole; they are real. The quintessential computer hacker, once dismissed as a solitary troublemaker or a teenage malfeasant, is today a technically sophisticated criminal who is often part of a larger, confederated crime operation. The motivation, today, quite simply, is greed. The rules of criminal hacking today are shaped by the economics of opportunity, incentive and risk – just like traditional theft, burglary or extortion.

One need only look at the highly sophisticated “phishing” scams plaguing the financial services industry – in which cyber criminals impersonate financial institutions and defraud consumers of their savings – to realize that we are not dealing with hobbyists or Robin Hoods. Indeed, the explosive growth in “phishing” is emblematic of the trends we are seeing in cyber attacks: a movement away from individual actors launching viruses and worms, towards highly sophisticated, transactional forms of Internet-based theft and fraud. These run the gamut from click-through fraud – which impacts 15% of all online advertising – to wide-scale identity theft. And while financial institutions have

been a prime and growing focus of these crimes, other components of our critical infrastructure, such as power and water facilities, have likewise been targeted.

This “professionalization” of cyber crime is unsettling for many reasons, not the least of which are indications that those who would seek to do harm to our nation have been working to improve their technological capabilities. Particularly unsettling is the real threat to the control systems and SCADA networks that monitor and regulate our nation’s industrial systems. Control systems are Internet connected, and are therefore susceptible to any number of malicious attacks. Under contract with customers, ISS has conducted real-world penetration tests with large power plants, oil companies, manufacturers and other users of control systems to demonstrate that these systems are indeed at risk to Internet-based attacks. Compounding the problem are Google type searches that demonstrate the degree of information available to would-be attackers on where and how to practice their procedures far away from the eyes of our government. The Internet offers criminals and other malicious organizations anonymity – the ability to commit crime remotely and in an untraceable way, or to use computer systems owned by others, as the vehicle to commit crime, house illicit materials or commit terrorist acts.

Put simply, Mr. Chairman, the fact that our nation’s critical infrastructure has yet to fall victim to a significant and coordinated cyber attack does not mean that it cannot happen. While I believe that our networks are robust and generally resilient, I nonetheless feel strongly that our critical infrastructures contain critical weaknesses that must be addressed.

Take, for example, the incidence of computer vulnerabilities: Despite the serious efforts of many technology companies post 9/11 to make their products and networks much more secure, the number of vulnerabilities that we are finding in computer systems today has actually grown -- not diminished -- since 2001. According to the Computer Emergency Response Team (CERT) Coordination Center, the number of known vulnerabilities climbed from roughly 2,500 in 2001 to nearly 6,000 in 2005. And in just the first half of this year, ISS has already documented almost 4,000 vulnerabilities. In fact, our world-renowned research and development team, the X-Force®, which tracks cyber threats and works closely with business and government to alert them of potential dangers, believes that we may reach as many as 7,000 published vulnerabilities this year – noting that this number does not include the number of known viruses, worms and spam. Disturbingly, the X-Force reports that June set a record for the most-ever disclosures of new computer vulnerabilities: 696 last month alone, meaning we are on track to find 42% more vulnerabilities in computer systems this year than we did last year. And since our critical infrastructures are essentially a complex web of interdependent computer systems, weaknesses in those systems can easily translate into weaknesses in our critical infrastructure. Case in point estimates are that 5-7% of Internet connected systems are currently compromised.

Part of the rapid increase in vulnerabilities may well be attributable to the fact that we as an industry are investigating vulnerabilities more aggressively than ever before. But that is not the whole story. The more likely answer lies in the fact that we have seen a

proliferation of new technologies in recent years – wireless, Voice over Internet telephony, and instant messaging, to name a few – whose security features are weak or even nonexistent. Emerging technologies and an exponential increase in the use of the Internet to advance business productivity, along with an exponential surge in the number of software applications used to conduct business, have opened many new avenues of attack. Keeping up with a large increase in vulnerabilities is a daunting task. We have seen and continue to track a shrinking window for the time a vulnerability is discovered to the time it is exploited by criminal interests. As the old saying goes, you rob a bank because that is where the money is. The Internet is certainly no different. The Internet Economy is the Economy. Today, that is where the money is, as well as the intellectual property, trade secrets or even the pathway to physical and economic disruption that those who wish to do harm can utilize.

The United States has the know-how to protect its critical infrastructure.

But there is good news, Mr. Chairman.

Our nation already has the technological capabilities to protect its critical infrastructure. Between the myriad of industry, academic, and governmental experts, we know where our cyber vulnerabilities lie; we recognize where are the back doors and open windows exist that provide entry points for cyber criminals and malicious threats, and we have the means and know-how to close them.

Take our own case, for example. As part of our mandate, ISS makes it our business to identify threats before they are exploited, and to arm our customers – including government agencies like the Department of Energy – with the tools they need to preempt these dangers. At ISS, we recognize our responsibility to share with governments and targeted industries worldwide the vast amounts of cyber intelligence we gather daily across our global networks and put this into useable formats. ISS employs technical experts whose sole responsibility is to work with governmental authorities and affected industries to apprise them of potential cyber threats. This responsibility extends to my level, Mr. Chairman. As an original member of the President's National Infrastructure Advisory Council (NIAC), I was pleased to contribute to the recent NIAC Intelligence Coordination Report and the NIAC Evaluation and Enhancement to Information Sharing and Analysis Report. The recommendations from NIAC to DHS contained in these reports are critical to strengthening the processes and protocols needed to prevent a serious cyber incident.

We work together, Mr. Chairman, because protecting our critical infrastructure is a job that the Federal Government cannot do on its own. The private sector collectively owns and operates at least 85% of our nation's critical infrastructures, which means that we must be our own first line of defense. Simply put, the Federal Government on its own cannot safeguard the most porous border there is – the Internet. That is a job for all of us.

Which is why countless public-private efforts to protect cyber space have arisen, including the Information Sharing and Analysis Centers (ISACs), which transmit cyber information intelligence between the private sector to the Federal Government; the Computer Emergency Response Team (CERT) Coordination Center, a Federally-supported, privately-administered clearinghouse for information about computer vulnerabilities; myriad protocols established between Federal agencies, such as the Department of Homeland Security, security developers like our own, vendors whose software they developed and important segments of our critical infrastructures; and more advisory boards, information-sharing councils, and experts groups than you can shake a stick at.¹

There is a point in vulnerability coordination where we can make great strides in providing protection to consumers across the globe. That point is after notification to the original equipment manufacturer (OEM) vendor and their ability to design an appropriate fix prior to public announcement. We know from anecdotal evidence that most organizations do not patch or upgrade their systems right away and that an overwhelming majority do not do so until somewhere between 30 and 80 days after public announcement. We also know that the criminal cyber attackers have new malware available within 24-48 hours after public announcement. Unfortunately, most of the security that all users have does not have a deployed fix available until about 24 hours later. Mr. Chairman, that means that many of our Internet users, government to business to consumer, are without any protection for days to months after attacks begin.

The know-how is there. The partnerships and protocols to harness this know-how are there, as well. The industry has the ability to coordinate amongst ourselves for all to benefit from better protection.

But what is missing, I am sorry to say, is genuine leadership on the part of the Federal Government to encourage us to do so.

Greater attention must be paid at the Federal level.

We as a nation can protect our critical infrastructure – in fact, we already are. But we can protect it much more effectively. And that requires Federal leadership.

By that I do not mean that the Federal Government should attempt to take charge of securing cyberspace. It is not possible, not to mention the fact that it would be an

¹ The long list of public-private efforts, as noted in the Business Roundtable's recent report *Essential Steps To Strengthen America's Cyber Terrorism Preparedness*, includes the President's National Infrastructure Advisory Council (NIAC), the National Security Telecommunications Advisory Committee (NSTAC); the Network Reliability and Interoperability Council (NRIC); the National Communications System (NCS) that operates within the Department of Homeland Security, along with its Alerting and Coordination Network; the National Cyber Security Division (NCSA), which includes CERT; and portions of the Homeland Security Information Network (HSIN), which is overseen by NCSA.

immense drain on resources to try to replicate the work already being done by a vast and diffuse network of private operators.

Instead, the Federal Government's role here boils down to one thing: *minding the store*. Working side by side with industry to shine a bright light on our nation's cyber vulnerabilities, helping to harness the resources needed to make sure that those vulnerabilities are addressed and encouraging the development of secure coding and strong computer architectures.

I appreciate and recognize the work that has been done by the Administration and the Congress to improve Federal cyber preparedness through initiatives such as the National Strategy to Secure Cyber Space, DHS' recently-announced National Infrastructure Protection Plan (NIPP), and the enactment of the Federal Information Security Management Act (FISMA). But I am sorry to say, Mr. Chairman, that despite these efforts, the Federal Government has fallen short in perhaps a more important way: The necessary leadership is not exercised on a day-to-day basis to place and keep cyber preparedness squarely on the national agenda.

Let me give you two examples:

First, it has been one full year since the Department of Homeland Security announced that it would elevate the responsibility for national cyber preparedness through the creation of the position of Assistant Secretary for Cyber Security and Telecommunications. And yet, one full year later, that position is still unfilled.

I recognize that it takes a while to fill sensitive jobs in Washington, Mr. Chairman, and I hesitate to put too much emphasis on a single vacancy when what is really needed is an integrated effort. But nonetheless, I believe that the fact that such an important role has remained unfilled for this period of time indicates a broader lack of urgency in many quarters of our nation with respect to cyber security.

I know that Secretary Chertoff and the Department of Homeland Security (DHS) are working round-the-clock to protect our nation. But with cyber security so integral to that protection, those of us who monitor, run, and own the networks that power our nation's critical infrastructure need to have access to a singularly-focused, authoritative point of contact. In short, we need to be able to talk to the person who is minding the store.

Secondly, Mr. Chairman, it is difficult for the Federal Government to preach strong cyber security practices across our economy when Federal networks themselves are so woefully unprotected. While steps have been taken in recent years to improve agency security practices, including through FISMA, most Federal agencies still get failing marks when it comes to securing their networks. And I mean this literally: we are all familiar with the cyber security report cards that Congress has given the Federal Government in recent years, in which most agencies have consistently gotten either unsatisfactory or downright failing grades. I wouldn't accept such marks from my children, and we shouldn't accept them from our government. Anyone who thinks the Federal Government is doing better

than these scores would indicate need only open the newspaper, which each day seems to bring a new story about lax practices leading to the disclosure of private or sensitive information.

Mr. Chairman, when it comes to strengthening Federal leadership in cyber security, we need five specific items:

1. The appointment of an Assistant Secretary for Cyber Security and Telecommunications empowered with the authority to establish and execute the Federal Government's cyber security strategy, which includes protecting its own networks and helping to ensure that those of the broader economy are secured. Portions of a Federal strategy have been outlined in various documents and action plans in recent years but without a single individual tasked with their execution, implementation has been spotty at best.
2. A clear delineation and hardening of the roles and responsibilities of the many public-private entities working today to secure cyberspace. There is simply too much confusion and, I suspect, duplication among the myriad of public-private entities laboring with the best of intentions in this space.
3. To ensure that the Federal Government makes full use of existing industry resources to gather and analyze data on cyber security threats. There is no point in DHS attempting to reinvent the wheel, which is what I fear sometimes occurs in well-meaning attempts at information sharing. The expertise needed to collect and analyze threats already exists in spades in the private sector; what does not exist are clear Federal processes for how to best make use of the private sector's analytical capability. The Federal Government must do more to encourage information sharing among those who already possess that information - the private sector - and utilize that collective knowledge.
4. A national plan to restore connectivity on a prioritized basis in the event of a large-scale cyber attack against our critical infrastructure. Contingency planning, disaster preparedness and recovery are, after all, quintessential government responsibilities. And while industry provides the pieces that form our critical infrastructure, it is the Federal Government that must help us pull these pieces together.

And finally:

5. Sustained Federal funding and active Congressional oversight to ensure that the Department of Homeland Security is doing all it can to harden both our nation's critical infrastructures as well as the Federal Government's own networks.

* * *

There is no silver bullet here, Mr. Chairman. Securing our nation's critical infrastructure from cyber attack requires a heightened degree of public-private coordination, information sharing, and trust than has been asked of us in most enterprises. Indeed, it is a challenge as unique as Internet itself. But it is one that I believe we as a nation are more than ready to take on, Mr. Chairman.

ISS is pleased to be a partner with you in this important effort, and I thank you for the opportunity to appear before you today.

Testimony of
Roberta A. Bienfait

Hearing on
“Cyber Security: Recovery and Reconstitution of Critical Networks”

July 28, 2006

Good Morning, Chairman Coburn, and members of the Committee.

My name is Robin Bienfait and I am the Senior Vice President of AT&T's Global Network Operations that includes the local, data and voice networks worldwide. In addition, I lead the teams that manage our 30+ Internet Data Centers, business continuity, network security, and disaster recovery for our global network.

I am responsible for the implementation of network design, development, engineering, operations, reliability, and restorability of AT&T's global network, and the deployment of new services, tools, and capabilities for next-generation Internet Protocol (IP) networks. On an average business day, AT&T carries more than 5.41 petabytes of data [peta = quadrillion]. That is equivalent to the printed contents of the Library of Congress in Washington, D.C. passing through our network every 4.6 minutes. AT&T also carries over 400 million long-distance, local and international voice calls on an average business day and we provide network services to 127 countries.

I joined AT&T in 1985 and have held a variety of technical and leadership positions of increasing responsibility over the years. I have led AT&T's international and domestic core network operations and technical support division and I have led the organization responsible for providing all domestic services for customers of AT&T Business, the company's largest operating unit. In the past, I also led an AT&T Labs organization as vice president for service assurance, electronic maintenance and IP/data systems. I also led an organization responsible for the fundamental development of critical underlying networking capabilities across all global services. I currently have 11 patents pending.

I want to thank you for calling this important hearing and for allowing me the opportunity to share with you what we have done and are doing generally to ensure the reliability and restorability of AT&T network services.

There are 3 keys to success in terms of network security and disaster recovery – and I will examine them today in the context of our experience with Katrina recovery and outreach and in the context of the black out of 2003.

Those 3 keys are: Preparation, Execution and Evaluation/Improvement

I will examine these three elements in the following ways:

- looking at the strength of the public/private partnership
- looking at lessons learned especially from Katrina and the power outage
- proposing a series of policy recommendations that we believe will move us all forward toward improving our national ability in all three areas

We believe that strong infrastructure protection and cybersecurity practices are good business and they are our highest priority.

The commerce of our country is supported by a cyber and physical infrastructure that is in effect a very closely coupled partnership between all of the providers and users of this infrastructure. In a very simple example a consumer internet banking service has infrastructure that includes servers provided by the financial institution, telecommunications facilities provided by AT&T, and the consumer's home PC & network. Federal, state and local government also have a role in this infrastructure partnership. All of the elements of this simple example have hardware, software, and other components that must be functioning correctly to provide the end service. Each partner has a responsibility to keep their part of the infrastructure up and working. They also each have a responsibility to be able to recover or restore their component of the infrastructure.

None of the partners should ignore their responsibility or they risk disrupting this closely linked partnership or more likely they risk becoming isolated from the other partners. One example of this type of isolation is related to consumer voice communication. More and more consumers are

relying on the very convenient and portable cordless phones or cellular phones as their only means of voice telecommunications. During the widespread blackouts on August 14, 2003 many of these consumers did not have a working phone due to the lack of power to charge the batteries required for their handsets. The lack of a functioning phone in the home could be inconvenient or it could be catastrophic to an individual if they needed to reach 911 emergency services. The voice communications network in the United States was functioning during the blackout but that really didn't matter to this subset of consumers. Mandating stricter recovery or resiliency requirements for the other members of the partnership would not have helped these consumers. There is a very important component of individual or enterprise responsibility to ensure the recovery of critical processes or functions. There are similar circumstances where large enterprises have the responsibility to protect their critical services and infrastructure that should not be abdicated to the other partners including the Government. AT&T recognizes the critical importance of reliable electrical power to our infrastructure operations. To protect our network and customers from interruption we maintain several layers of emergency power backup. We do not assume that the electrical utilities will always be able to provide us the electrical power we need to operate our infrastructure.

For the fifth consecutive year, AT&T has polled chief information officers and other senior IT executives at companies throughout the United States with more than \$10 million in annual revenue for their views on disaster planning/business continuity trends. Despite the devastating effects of Hurricanes Katrina and Rita last year, nearly half of the 1,000 companies polled by AT&T also said that they do not take specific protective actions even when state or federal governments issue warnings for an impending disaster, such as severe weather. It's evident that for some companies, the various events of the past year have been a real wake-up call. That's the good news. But it's surprising how many companies are still putting their businesses and future at risk by not adequately planning for the next hurricane, earthquake or cyber-security hit.

AT&T takes our responsibility for operating secure and reliable networks very seriously. Our network design goal is to have a network where failures are prevented, or predicted and pro-actively corrected, before they impact a customer's service. This goal is the foundation for the preventive, predictive, and proactive efforts that we take to first protect our physical and virtual infrastructure and second to be able to restore this infrastructure under any circumstances.

I. PROTECTING CRITICAL COMMUNICATIONS INFRASTRUCTURE

A. Preparation

As a preliminary matter, there are three overarching steps that AT&T has taken – and that are essential to protecting vital communications infrastructures. The first begins long before any disaster occurs. It entails *preparation* to ensure that the network and its components are as reliable as possible through proper design, hardening, redundancy, and performance at levels that far exceed routine needs. At AT&T, for example, we engineer our network to “five nines” of reliability – 99.999% reliability – that requires a diversity of communications links and equipment. This measurement relates to the number of defects in relation to opportunity. For every million opportunities 10 defects equal 99.999% availability/defect free or “Five Nines”. For example, if you have 400 million calls during a given day, 4,000 blocked calls is equivalent to 99.999% were completed. Another example would be if 10 million packets were sent, if 100 were dropped, this is equivalent to 99.999% were successful or “Five Nines” performance.

When links and associated systems fail, there must be instantaneous and seamless rollover to backup facilities. This capability must be periodically tested, and given the frequency of cable dig-ups throughout the country, let alone emergencies of unprecedented scale such as Katrina, this testing must occur frequently.

Proper preparation, however, also contemplates that even the best facilities could fail. Proper preparation therefore requires rigorous planning for service restoration, including advance placement and availability of service restoration equipment where it can quickly meet identified needs, and ongoing training to ensure the availability of the skilled workforce needed to restore service. We make restoration our first priority and then move on to make repairs.

- Such a commitment to preparation, excellent service in the face of disaster, and responsiveness to threats to our networks and customers, does not come cheaply. At AT&T, we have invested over \$300 million since 1991 in our mobile Network Disaster Recovery (“NDR”) infrastructure and capabilities. We also invested \$200 million in an AT&T Labs-developed system called I-

GEMS that proactively monitors and manages the networks of some of our largest customers. We bring our Emergency Communications Vehicles ("ECVs") wherever needed to provide communications services in an emergency, and we have more than 500 various vehicles stored in locations around the country and loaded with generators, fiber and other supplies, repair and restoration facilities, circuit and packet switching, HVAC capabilities, lights, batteries, chillers, pumps, food, first-aid and whatever else may be necessary to make our response effective. We have the basic building blocks of our network infrastructure hardware and software installed in 150 technology trailers including the same electronics and optics that are installed in our telecommunications hubs. This equipment is installed and ready to roll at a moments notice. Our NDR can be seen as an active extension of our network that stays powered up and in synch with the 'live' network. We have extensively drilled our teams in various scenarios on a quarterly basis to ensure that readiness remains at peak levels.

Our Business Continuity/Network Disaster Recovery disaster planning and Continuity of Operations Plan ("COOP") gives us the ability to duplicate necessary capabilities quickly to meet or exceed our customers' business needs and continuity requirements, including those of our government customers. This has many components, including unparalleled security capabilities, logical systems, and physical capabilities. Network security is of particular importance given the prevalence of attacks through worms and viruses and the possibility of related threats. AT&T works diligently to provide network security for our infrastructure and to our customers. Network security requires great focus and attention, and will certainly remain a critical challenge.

AT&T also established a system level Certification and Assurance governance process whereby we measure our estimated likelihood of recovery in the event of an incident. We then drill down to the component level and assess the consequences of a potential failure and the impact to our business. We work to mitigate the risk of failure by either eliminating the threat and the vulnerability,

or by mitigating the exposure. This process informs our rigorous business case analysis and brings clarity to investment decisions. We regularly assess these components both for ourselves and on behalf of our customers.

An extremely important part of our preparation is focused on the virtual element of our infrastructure. Like every enterprise, AT&T faces multiple and growing threats to information security. Software viruses, Internet worms and denial of service attacks have become common. "Phishing" schemes aimed at extracting personal information from unsuspecting users appear every day. Much of what attempts to enter the corporate intranet is made up of unsolicited commercial messages, or spam. According to AT&T security experts, more than 75 percent of the e-mail messages aimed at the att.com portal daily are spam. Intelligent network security functions require infrastructure, analysts and expertise. We are the only provider that maintains an active research laboratory. The algorithms that we have running in our database are all proprietary, they're all based on sifting through daily traffic and trying to find anomalous conditions. By keeping a laboratory, by having infrastructure that we build up over a period of time, we can demonstrate the feasibility of these types of security techniques, methods and algorithms with our customers.

Like most large enterprises, AT&T was using a system of premises-based security firewalls distributed across the company's many locations. The company reviewed several options. As discussions continued, the most effective and efficient solution emerged: a solution based not solely on the company premises, but a layered approach with an emphasis on leveraging the network. In early 2004, AT&T security planners initiated a more comprehensive and systematic approach to security planning and implementation. How do we utilize the inherent strength of AT&T's network, they asked, to create security solutions that meet our internal needs and also meet the needs of our customers? Why not move many security defenses out of company offices and into one network that ties all those sites together? In addition to fending off attacks and providing more consistent software

patching, AT&T's security approach is designed to assure business continuity. Security infrastructure equipment is housed in hardened AT&T data centers, disaster-ready buildings equipped with robust backup systems, instead of being dispersed at potentially more vulnerable enterprise sites.

AT&T has a portfolio of security services that protects customer's vital data and secures their enterprise networking environment. AT&T delivers a suite of offers that assess vulnerabilities, protect customer's infrastructure, detect attacks and respond to suspicious activities and events. A leading innovation that came from the company's own learnings is AT&T's service called Internet ProtectSM Service. This security alerting and notification service offers advanced information regarding potential real-time attacks including viruses, worms and DDOS attacks that are in the early formulation stages.

B. Execution

The second vital step to protect communications infrastructure requires *execution* during and immediately following a disaster. In many respects, execution is a function of proper preparation, particularly having a robust infrastructure, a well-trained and frequently-drilled workforce, and facilities and capabilities available for service restoration. Effective execution also requires a sophisticated command and control structure in emergencies to make every minute count, every deployment as effective and efficient as possible, and to enable our dedicated employees to work as safely as possible. We follow an incident command structure, which is led at every moment by an experienced Executive Duty Officer. Our incident command structure is a variation of the same National Incident Management System (NIMS) that is an important part of the National Response Plan under DHS. It is used by many other first responders in the public and private sectors. We do not wait for disasters or other emergencies to use our incident command system. As a foundation discipline we use it to manage changes in our network hardware & software and to manage other network incidents like fiber cable cuts. This allows our team to use the process on a regular basis so during a disaster it becomes a much more focused second nature.

In addition, execution requires close coordination with third parties, including federal, state, and local government authorities and first responders, others in the telecommunications industry, and others in the private sector trying to restore essential services and facilities, such as power, water, roadways, and the like. This communication and coordination effort is often the most difficult part of execution during and immediately after a disaster. In the communications field, the telecommunications industry response to disasters, other than that of a company responding to damage to its own facilities, is typically coordinated through the National Coordinating Center for Telecommunications ("NCC"). The NCC, as part of the Department of Homeland Security, has an important role in the telecommunications industry's ability to continue to operate our telecommunications infrastructure after a disaster by acting as a liaison between the industry and the government. They match telecommunications companies to those governmental entities with unmet emergency telecommunications needs. The NCC also provides a means for the telecommunications industry to request the assistance of the Federal Government. We have assisted the Federal Government and other carriers after receiving requests through the NCC including helping the Federal Marshals establish satellite communications in NYC after the WTC attacks. We have also received assistance from various Federal agencies after requesting it through the NCC including: fuel assistance after Tropical Storm Allison in 2001, flying a few of our NDR team members on a military transport from California to New York after the attacks on 9/11, and flight path requests for our helicopter support after Hurricane Katrina.

Finally, execution requires ingenuity and resourcefulness when the unforeseen happens. Each emergency situation presents its own unique set of challenges. Even the most thorough planning and training cannot take the place of highly skilled and resourceful emergency responders who can recognize and adapt to unplanned circumstances.

C. Evaluation and Improvement

Finally, the protection of the communications infrastructure requires a thorough and frank after-the-fact evaluation of performance, distillation of lessons learned, and implementation of *improvements*. In this regard, one outcome of Hurricane Katrina should be a critical reassessment of our performance as individual communications companies, as an industry, and as a nation, and implementation of the policy recommendations needed to improve performance in the future.

II. IMPACT OF KATRINA ON THE NETWORK AND ITS RESTORATION

Overall, AT&T's network remained overwhelmingly intact following the hurricane and flooding. At all times, we were able to carry at least 95% of the calls in the Gulf Coast area that came to our network. Of the 5% of our capacity in the area that was initially lost, FASTAR ®, our software and hardware system that redirects and reroutes traffic, restored half of that capacity within a couple of hours. Within 24 hours of the storm making landfall, another quarter of that capacity was restored via manual rerouting, and the final quarter was restored within 48 hours of the storm making landfall when AT&T workers physically installed two cables in the ground and rerouted certain traffic. This latter effort successfully worked around the loss of certain regenerators that boosted the strength of digital bits long distances over fiber. On a nationwide basis, on the day of Katrina and over the next few days, we successfully carried intercity traffic at levels that exceeded demand the week prior to Katrina by approximately 10%.

Nonetheless, because we interconnect with other carriers, including local exchange carriers and wireless carriers, we could not complete calls to other networks that suffered more severe disruptions. As a result, following Hurricane Katrina's landfall on the Gulf Coast, we needed to block millions of calls a day into the affected area due to outages in other telecommunications carrier's networks.

We built our only major switching station in the New Orleans area on high ground utilizing "submarine doors" and, therefore, it was not flooded. We had also invested money in the infrastructure of this major switching station based on past flooding threats in New Orleans including moving critical electrical equipment and emergency generators to upper floors in the facility. One of our most immediate concerns in the aftermath of Katrina regarding that facility, however, was looting

and security. Security concerns forced employees to evacuate our switching center late in the afternoon on August 31st as local law enforcement was unable to ensure the safety and security of the site. We requested the assistance of DHS and they dispatched heavily armed U.S. Marshals and FBI Special Agents to secure our critical switching center early that evening. Our employees returned to the building the following day, together with BellSouth employees who worked in the same building. They were escorted into the area by more U.S. Marshals and FBI Special Agents provided by DHS. At that time, our people delivered to the building fuel for the generators, water for the air conditioning chillers, food, and other supplies. Law enforcement authorities also set up operations in the lobby of the building in order to utilize the telephone connectivity available there. During the period that our employees were out of the building, the network infrastructure was put on automatic controls and monitored remotely by the AT&T Global Network Operations Center.

We had 162 offices loose commercial power during the storm event. We had ensured a sufficient backup generators and enough fuel for them. We were able to restore power by putting many of these sites on generators, and by making use of batteries or fuel cells in connection with a few. We replenished fuel supplies as necessary to avoid disruption, but our preparations included staged supplies of thousands of gallons of gas in portable containers, thousands of gallons of diesel fuel in portable cells, and thousands of gallons of water in portable tankers for cooling towers.

III. AT&T'S KATRINA RESPONSE AND OUTREACH

AT&T began moving equipment and teams from around the country toward the Gulf States in the days before the storm made landfall. We followed our prescribed approach. The first team restored AT&T's service to its prior levels, the next maintained and monitored AT&T's facilities so as to prevent new issues from arising, and the third came in to help others. AT&T worked around the clock to respond to this crisis and safeguard its network, support efforts to respond to the disaster, and address the needs of evacuees.

Because we fully restored and secured all of our network capabilities within the first 48 hours of the crisis, in a spirit of service and compassion, AT&T was able to direct its efforts to benefit its customers, other telecommunications competitors and their customers, first responders, and evacuees as needed. In this instance, we were largely able to use our in-place capabilities to meet not only our own needs, but also those of others. We put a variety of our facilities to work for other carriers and their customers, and continue to carry significant amounts of additional traffic for other carriers that cannot currently do so themselves. AT&T also helped to provide relief to those directly affected by the hurricane and flooding, and assistance to charitable relief activities.

Of course, the same is particularly true of our work with government customers like FEMA. In addition to immediately increasing FEMA call capacity and toll-free number availability, over the weekend of September 10th, AT&T was able to install an additional 3,360 voice circuits to boost call center capacity to support FEMA. AT&T worked directly with the IRS to execute in less than 24 hours an agreement to direct calls using IRS trunks which IRS provided to give FEMA necessary increased call capacity.

At the same time, we coordinated with the DHS NCC regarding the considerable resources that we could make available. First, we focused on the broader telecommunications network and the critical needs of first responders and ongoing rescue operations. In coordination with the NCC, we dispatched five Emergency Communications Vehicles (“ECVs”) with satellite capabilities, and other forms of assistance, to assist in the relief efforts. Never before had we deployed so many of our satellite assets to a single area. During the first 13 days of the crisis, over 104,000 calls were made through AT&T ECVs. We assisted the Louisiana State Police, the Louisiana National Guard, Stennis International Airport, NASA and others, including civil emergency communications authorities in Mississippi and Louisiana. We also provided some of our portable diesel-powered generators to Louisiana State Police Troop L headquarters in Mandeville, LA on Saturday morning, September 3. They had lost their back-up power generator that morning. We offered an AT&T generator until its own could be repaired or commercial power restored.

The second part of our response was to provide relief to individuals, telecommunications services in support of charitable work, and to make our own charitable contributions.

- Working with Avaya, Cisco and SBC, we helped establish a communications network for evacuees at the Astrodome, including more than 1000 phone lines as well as data infrastructure.
- We established a phone bank to assist displaced college students to find alternative educational opportunities.
- We provided toll free calling and 10 call centers for a successful fundraiser: “Shelter from the Storm: A Concert for the Gulf Coast.”

- The AT&T Foundation also pitched in to address the needs created by this disaster. It donated \$1.5 million¹ and 148 laptops to the Red Cross for relief efforts. It issued 35,000 pre-paid calling cards for distribution to survivors and evacuees.

¹ This figure includes \$500,000 in matching funds for donations from AT&T employees.

IV. IMPACT OF 2003 NORTHEAST BLACKOUT ON THE AT&T NETWORK

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. This outage affected an area with an estimated 50 million people in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm Eastern Daylight Time and power was not restored for 4 days in some parts of the United States. Estimates for the cost of the blackout range between \$4 billion and \$10 billion with the U.S. Department of Energy estimating \$6 billion.

Internet traffic, data services, and voice calls flowed across our network without interruption. This was not due to luck but instead the reliability and redundancy that we designed and built into our network infrastructure including the multiple layers of emergency power provided by generators and battery back-up. It is also a tribute to the people of AT&T who worked around the clock to keep America's communications infrastructure up and running. We used our very disciplined incident command system to manage the event including refueling of some generators, moving portable generators to charge batteries at some of our smaller fiber cable regenerator stations, and respond to assistance requests from other carriers and some of our customers.

282 of our Network nodes were protected by our emergency backup power infrastructure for intervals ranging from several minutes up to 74 hours. AT&T did experience a significant spike in our long-distance phone traffic after the initial outage, which leveled off during the night. Our network performed superbly during this voice call surge and the call levels were back to normal by the next morning.

We did have a problem with one of our local voice switches in New York City on August 14th when the landlord at one of our leased facilities refused to let us run a standby generator that we had for emergency backup due to exhaust fumes that were drifting back into the building. Late that evening the backup batteries for the site exhausted and we lost power at this location. By the time the batteries had exhausted and we lost power the business customers that were served by this voice switch had already left the city. We requested assistance through the New York City Mutual Assistance Restoration Consortium (MARC) to get a NYPD escort for a portable generator we brought in to provide power. The police escort was required to bring the generator through the gridlock caused by the blackout. NYC MARC has a very similar mission to the DHS NCC and acts as a two way liaison between the local authorities and private industry infrastructure operators including power, gas, and telecommunications.

IV. LESSONS LEARNED

Each emergency situation presents its own unique set of challenges, and even the most thorough planning cannot take the place of ingenuity and resourcefulness when the unforeseen happens. That said, much can be anticipated and we must plan and drill to address a variety of events on any scale. I am sure I join all of you in saluting our first responders and relief workers in their tireless efforts. But the importance of resourcefulness does not in any way obviate the need for very carefully thought out emergency planning led by seasoned professionals.

Our experiences have reinforced the following lessons which we all must incorporate in future planning:

- **Establish and Practice Disaster Recovery Processes in Anticipation of Emergencies: Communications, Command and Control.** Communications resources can be brought where needed very quickly, but it is essential that there be clear lines of command and control at all times in order to direct those resources effectively and to the area of greatest need. Moreover, if because of the scale or nature of the disaster, some aspect of the plan affecting the command structure is not workable, an alternative must also be part of the plan and ready for implementation. Finally, without practice and drilling, no team will be ready and no plan will be ready to implement.
- **Internalize the 3P Paradigm: Preventive Action, Proactive Focus, Predictive Models.** It is crucial to invest in facilities and plan and drill regularly and thoroughly for a wide variety of contingencies. Investment cannot be deferred and possible scenarios ignored. We cannot wait for a disaster to occur before we are prepared to move aggressively.
- **Make Risk Analysis Routine: Harden Critical Infrastructure Where Indicated.** It is imperative to know what part of your infrastructure is critical to continued operation of the network in times of crisis and how to harden it as much as possible and to replace or restore it to the extent it may be damaged. Such analysis must be part of any risk assessment, and the assessment must be followed promptly by action.

- **Establish Crisis Management Plan.** Every emergency situation is different, and even the best planning may not prevent things from going wrong. Thus, we need to prepare ourselves for that eventuality. Crisis management plans must recognize and allow for improvisation to adapt to the given circumstances.
- **Coordinate Restoration and Recovery Effort.** There should be no wasted effort in recovery operations. Everyone available should be participating, and there needs to be coordination so that efforts are not duplicated or in conflict with one another. The NCS NCC played a very positive role in matching available resources to pending needs. It is essential that logistical information such as what roads are closed and what medical precautions need to be taken be readily available. Moreover, a recommendation we made after 9/11 still has not been widely implemented. Companies who are crucial to the response to disasters such as AT&T should have special credentials designed for employees and accredited in advance in order to access disaster areas. In some cases AT&T employees only were able to respond and move mobile resources into the Gulf Coast area by virtue of their resourcefulness in talking their way into affected areas. Letters were provided during the disaster response but not all state and local law enforcement authorities recognized or honored them.
- **Design Five 9's of Reliability.** This storm again confirmed that telecommunications companies that design their networks to this standard – 99.999% reliability – have excellent disaster recovery and response capabilities, as well as reasonably hardened networks. That is the only way to maintain this standard. In times of crisis, this capability becomes a vital national asset.
- **Interoperability and Spectrum Availability.** A crisis on the scale we saw in the Gulf Coast, and smaller challenges as well, demand a well coordinated information and communications delivery system. We must resolve the spectrum needs highlighted by the 9/11 Commission, among others, to provide first responders and others with a better and more effective means of communicating quickly and easily in an emergency.

POLICY RECOMMENDATIONS

These lessons learned lead to the following specific policy recommendations:

- Focused and unified incident command is a very important function for coordinating any type of event but would be absolutely critical during a massive, nationwide disruption of our shared cyber infrastructure. The FCC, DHS Office of Cybersecurity & Telecommunications, National Cyber Response Coordination Group (NCRCG), and the NCC all appear to have roles in coordinating any reconstitution of the internet after a massive outage. A single agency must be identified, funded, and empowered to act as the National Cyber Incident Commander for any required cyber infrastructure recovery and reconstitution efforts.
- The agency that is designated as the National Cyber Incident Commander must also be the lead for the planning and exercising of coordinated response plans with all parties in the cyber infrastructure. The first items that must be addressed immediately by this agency are a coordinated advanced warning mechanism including an emergency communications plan. The coordinated advanced warning mechanism should be a way of identifying potential emergencies and agreed-upon protocols and thresholds that indicate an attack is under way or a disruption is imminent. Something along the lines of a blend between the Centers for Disease Control and Prevention (CDC) and the NOAA National Hurricane Center for our cyber infrastructure. An emergency communications plan must address the protocols and processes for responding to severe failures as well as the infrastructure used to communicate. This infrastructure could be a blend of the recently dissolved Alerting and Coordination Network (ACN) and the SHared RESources (SHARES) High Frequency (HF) Radio Program administered by the NCC. This emergency communications infrastructure must not rely on the underlying cyber infrastructure. In the absolute worst case scenario of a complete cyber infrastructure shutdown the best communications means to coordinate the recovery and reconstitution may be a private line conference bridge arrangement or even HF radio.
- Drill frequently for emergencies under various scenarios and include the public and private sector. Do not be satisfied with a written plan. Put the plan in practice and continue to improve. A plan that is not tested and exercised regularly can actually be more harmful than not having a plan. A false sense of security is created with the untested plan and usually many resources have gone into producing something that may never work in trying circumstances.

An honest and thorough after exercise evaluation of performance, distillation of lessons learned, and implementation of improvements.

- Furnish standardized and approved emergency credentials to vital communications and other infrastructure providers in advance, so that AT&T and other specialized disaster staff can get into affected areas to restore vital capabilities without delay or interference. While our teams were given letters from state officials authorizing them to enter impacted areas, those were not necessarily recognized by security and other law enforcement personnel in the field. We have been participating in a trial of the DHS First Responder Authentication Card system that appears to meet this need. A national credentialing system must be established to allow us to more quickly restore critical communications after a disaster or other emergency.
- Predetermine security needs and formalize request process from telecommunications carriers for law enforcement deployment to protect critical infrastructure facilities immediately following a disaster.
- Increase the visibility of the resources that our Government has already created for emergency planning. www.ready.gov is an excellent resource provided by the DHS that includes emergency planning advice and resources for our citizens, businesses, and even our pets to help us all prepare for the unexpected. It should be promoted more widely to promote the message of individual and enterprise accountability for disaster and emergency planning.
- Consider subsidizing some emergency preparation by infrastructure companies since the government is likely to call such capabilities into use or would otherwise need to duplicate resources inefficiently.
- Minimize the amount of regulation and data reporting requirements during a disaster and maximize the amount of coordination and cooperation between the public and private sector. The priority must be on the safety of our employees and the recovery and reconstitution of this critical national resource. The limited Special Temporary Authority (STA) and waiver of the FCC's rules to engage in integrated disaster planning and response without observing the FCC's structural separation requirements that was granted by the FCC to AT&T, and several other carriers, is an excellent example of focusing on the recovery mission.

We can never anticipate every contingency in an emergency, nor can we assure a foolproof communications network all the time under all circumstances. Nonetheless, at AT&T, we have done much to ensure reliability and restorability of communications networks and together – as an industry and as a nation – we can do more. I thank you for holding this hearing to advance this important discussion.

* * *

161

Before the
Subcommittee
on Federal Financial Management, Government Information and
International Security

Committee on
Homeland Security and Governmental Affairs
United States Senate

“Cyber Security: Recovery and Reconstitution of Critical Networks”

Statement of
Michael A. Aisenberg, Esq.
Director of Government Relations
VeriSign, Inc.

Washington, D.C.
28 July 2006

Statement of Michael A. Aisenberg, Esq.
Director of Government Relations, VeriSign, Inc.

Mr. Chairman, distinguished members of the Subcommittee, my name is Michael Aisenberg. I am Director of Government Relations at VeriSign, the California-based Internet infrastructure company. I am also Vice Chair of the new IT Sector Coordinating Council, engaging with DHS on cyber security policy, and am chair of the President's NSTAC International Task Force, the ITAA Information Security Committee, and a Board Member of the IT ISAC.

I have a prepared statement which I would ask be included in the record in its entirety. My remarks today are those of VeriSign, as a corporate member of the cyber infrastructure community.

Mr. Chairman, I appear here today after a career of thirty years of translating from the "tech" to the "Congressional." My entire career, including my years in government, has largely been spent working with the legislative and executive branches, on behalf of IT companies.

Today, and for the past six years, I do this work for a core Internet infrastructure company. Based in Mountain View California, VeriSign is a company of over 3500 employees, who operate intelligent infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. VeriSign currently secures over 450,000 Web sites with digital certificates—including sites for 93% of the Fortune 500. Today, the VeriSign Secured Seal appears on over 34,000 sites worldwide, a ubiquitous symbol of trust. VeriSign facilitates over 18 billion Internet Domain Name queries every day, and can support many times that amount, should RFID tags replace the current barcode system, filling networks with timely product information. VeriSign operates the largest SS7 network in North America, securely routing 2.7 billion phone connections every day from carrier to carrier, across national boundaries, and between protocols. We are the largest mediator of cellular roaming services in North America, and support cellular carriers with the largest inter carrier billing system. We are deeply involved in the development of policy within our sector and at the national level. Our Chairman, Stratton Sclavos is a member of both the President's Council of Advisors on Science and Technology and the President's National Security Telecommunications Advisory Committee, where I am privileged to chair the newly established International Task Force.

Mr. Chairman, I am pleased to be present with distinguished colleague companies, and in particular, with a representative of the BRT, which has recently published its views on DHS' management of cyber security. This document is important, because its conclusions are largely correct and widely shared.

I would like to make three important points today. First, those who make policy in the United States must understand the economic value and critical interdependencies we have developed on our information networks. Second, we must understand, acknowledge and accommodate to both the global nature of our information networks, and the threats and continuing attacks being mounted against them. Third, the security of our networks, largely owned and operated by the private sector, depends on effective partnership between government security, intelligence, law enforcement and user agencies, and the private sector stewards of these infrastructures.

Allow me to elaborate.

Americans must appreciate and keep a clear focus on the critical economic and national security role which our information networks have come to fulfill over a very short period. In less than two decades, this country has evolved an irreversible dependency, and interdependency by America's banking, finance, transportation, health care, education, power, manufacturing and government services on the networks managed by the companies which make up the IT and telecom sectors.

Each day, 3 trillion dollars worth of economic activity pass over secure Federal financial networks. Securities sales settlements, check clearances, interbank transfers. That is nearly 1/3 of our Gross Domestic Product. If these electronic transactions do not have Internet sites such as NYSE.Net, BankofAmerica.com and Treasury.gov available, secure and running, U.S. economic activity begins to grind to a halt, at the rate of \$130 billion dollars per hour. So cyber security-- the function of safeguarding both the physical and logical infrastructures which enable this economic activity-- is an essential activity of DHS, and of the rest of the U.S. national security community. Cyber security is indeed a responsibility which we all share and in which we all have a stake.

Second, we must lose our cyber nationalism and phony techno-xenophobia. The United States—government and industry--must recognize that these information networks are global, and are managed in increasing measure by interests outside of the control of the U.S. government. At the same time, our networks are being subjected to threats and attacked by actors from around the world.

As we reach 200 million North American Internet users by the end of this decade, the rest of the world will pass two billion users. Unquestioningly, we in the U.S. originated much of the underlying technology, the computer and network hardware, and the complex protocols and network software on which the global network depends. But while we have "carpet bombed" the planet with this technology, we can no longer claim exclusive dominion over it. Networks are largely agnostic about national borders. The U.S.—industry

stewards of critical infrastructure and the government-- must work globally within public and private sector mechanisms to evolve governance models which retain necessary and appropriate links between U.S. national security, defense and law enforcement interests, while accommodating the legitimate aspirations of governments and network users around the world to have a stake in the operation and evolution of tools that shape their own social and security futures.

Third, the role of an effective government cyber security actor and government-industry partnership is central to the maintenance of the critical security posture protecting cyber networks. It is important we not lose sight of the BRT report's critical conclusion: we need a much improved cyber security activity, not just in DHS, but across government interests.

The global threats mentioned earlier are not slowing, but accelerating. They are not becoming limited, but rather, are growing in scope and scale. They are not becoming trivial, but much more sophisticated. All of these facts mean the overall risk is growing, and for every security solution we put in place, we can expect our adversaries to develop an attempted "trumping" assault. This is much like a cyber arms race, with no end likely to be achieved.

But the BRT's suggestions about the extent of private industry engagement with DHS, especially over the past eighteen months, are, I believe largely incorrect and out of touch with the facts of important progress being made in public-private collaboration specifically directed at improving the admittedly risky national cyber security environment.

In the last eighteen months, we have seen DHS make significant and important progress in migrating from a frankly dismal posture in 2003-04 when Cyber Security was demoted out of the White House and into the lower rungs of a new agency, to a substantial, active entity engaging effectively with industry on many fronts.

Beginning with the TopOff III exercise planning in the fall of 2004, a steady improvement and expansion of industry involvement with DHS' cyber and network security activities has been evident. This improvement must continue.

The TopOff III exercise occurred in the spring of 2005 with less-than-desirable cyber and telecom sector participation. At about the same time, early drafts of the National Infrastructure Protection Plan or "NIPP", devoid of any meaningful discussion of the cyber infrastructure were released, and thankfully, promptly pulled back. These represent the low points.

Comment from industry on these processes began to be sought by new DHS leadership. Private sector involvement in DHS' policy process from their

beginning, rather than at the end, long an aspiration of those of us representing industry through our organizations, began to be practice.

The national cyber security exercise, Cyber Storm, which occurred in February, included extensive sector participation in its planning, and was a remarkable success as a learning experience in public-private cooperation. Led by the IT ISAC, the IT sector gained valuable experience in Cyber Storm, and a new impetus toward the development of a concept of emergency operations for the sector.

DHS' multi stakeholder Internet Disruption Working Group (IDWG) was developed in 2005 and culminated in a day-long planning conference in November, and a recent valuable and widely attended day-long table-top exercise last month, involving DHS and other security agencies, other Federal and sub-Federal government interests and a wide range of private sector cyber infrastructure organizations.

The government's security operations community, GFirst, held its annual conference in Florida in May, which was widely attended by dozens of private sector representatives as well as hundreds of government network security managers, and accompanied by a day long engagement between senior staff or the U.S. CERT and the IT ISAC's con ops task force.

The NIPP has just been released, over the signatures of Secretary Chertoff and 14 other Cabinet members. The NIPP, as a framework for action, including public-private collaboration, incorporates extensive views of the IT and telecoms sectors, and explicitly reflects a focused recognition of the cyber sector's structural and operational differences from physical critical infrastructures, both in the NIPP text and in the separate Cyber Appendix.

The IT and Communications Sector Specific Plans contemplated as operational components of the infrastructure protection process are now under development in a full partnership model between industry representatives and DHS and other GCC member agency representatives. The process is thoughtful, effective, and may well be exemplary for other sectors' SSP development.

These milestones in improvement in the relationship between cyber sector industry interests and the NCSD and NCC staff are important and significant. They are, however, not a solution, but a beginning. This is because cyber security is indeed an ongoing process, and because, as GAO reports so often state, "Progress has been made, but much remains to be done."

Indeed, many of us believe that notwithstanding these improved engagements between the public and private sectors, the actual operational posture of the cyber sector and DHS' is still fraught with risk. It has been observed that if a

9/11 like attack were to take down the NYSE today, (putting aside the issue of improved back-up sites) there is simply no way that the NYSE could restore its network dependent functions in the same four days it did in 2001, and indeed, perhaps not in four weeks.

And the principal reason for this unlikely prompt restoration is DHS, or rather, the bureaucratic impediments to the kind of nimble, self-motivated, selfless action that dozens of private sector entities engaged in 2001 to bring the exchanges back on line. Katrina has amply illustrated these problems; we should not wait for a 2006 hurricane season test of post-Katrina lessons-learned to determine if our economic and other network dependent infrastructures are supported by a necessary government structure, to facilitate private sector action. We need to act without delay to assure that our networks and the critical sectors dependent on them are resilient enough to withstand the attacks being mounted against them each day. And our critical networks must be supported by the appropriate tools from government as well as industry to assure the ability to recover from disabling attacks with minimum collateral impact on our economy and security.

Several steps are necessary to assure this.

First, DHS' modest cyber security budget must be insulated from the continuing reprogramming and budgetary cuts now underway. There will be neither a virtual Bourbon Festival OR Nick's Online Check Cashing if there is no Internet.

Second, a cyber security leader with credibility in industry and within the Federal cyber community must be identified and appointed as DHS' permanent Assistant Secretary for Cyber security and Telecommunications without further delay.

Third, critical R&D projects directed at improving the key security protocols of the Internet must be funded and launched or relaunched, on a fast track basis if possible.

If we do these things, we will not guaranty that our adversaries will stop attacking our critical cyber assets, but we will improve the likelihood that we will successfully withstand those attacks, and retain the availability of these infrastructures on which we are now so dependant. Thank you Mr. Chairman, and Mr. Chairman, I will be happy to answer any questions.



Business Roundtable

*Strengthening America's Cyber Preparedness: Essential Steps for the
Public Sector and the Private Sector*

*Before the Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government
Information, and International Security*

July 28, 2006

Karl Brondell
State Farm Insurance Companies
on Behalf of Business Roundtable

Testimony and Comments for the Record

Business Roundtable
1717 Rhode Island Avenue, Suite 800
Washington, D.C. 20036
Telephone: (202) 872-1260

Introduction

Thank you for this opportunity to testify today on Internet recovery on behalf of State Farm Insurance Companies and Business Roundtable.

Business Roundtable (www.businessroundtable.org) is an association of chief executive officers of leading U.S. companies with over \$4.5 trillion in annual revenues and more than 10 million employees. Our companies comprise nearly a third of the total value of the U.S. stock market and represent nearly a third of all corporate income taxes paid to the federal government. Collectively, they returned more than \$110 billion in dividends to shareholders and the economy in 2005.

Roundtable companies give more than \$7 billion a year in combined charitable contributions, representing nearly 60 percent of total corporate giving. They are technology innovation leaders, with \$86 billion in annual research and development spending – nearly half of the total private R&D spending in the U.S.

Following the 9/11 attacks on the World Trade Center and the Pentagon, Roundtable CEOs formed the Security Task Force to address ways that the private sector can improve the security of employees, facilities, communities and our nation. The Roundtable believes that the business community must be a partner with government in disaster preparedness and response because more than 85 percent of the nation's critical infrastructure - power grid, financial services, information services, railroads, airlines and others - is owned and operated by the private sector.

The Roundtable commends the Subcommittee and its members for their interest in improving procedures and preparedness to ensure recovery of the Internet following a major disruption. Hardening the Internet and strengthening cyber security is one of the priorities of the Security Task Force, which is chaired by Frederick W. Smith, Chairman, President & CEO, FedEx Corporation. The working group focusing on cyber security issues is led by State Farm's Chairman and CEO, Edward B. Rust, Jr.

Preparing for Internet Recovery

More than a year ago, the Roundtable began work on an initiative to assess the public sector and the private sector plans and procedures for Internet recovery following a cyber catastrophe. We have just produced a report, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness*, which identifies significant gaps in our nation's preparedness. The Roundtable has provided copies of our report to the Subcommittee, others in Congress and to the Department of Homeland Security.

The Roundtable's analysis finds that the United States is ill-prepared for a cyber catastrophe, with significant ambiguities in public and private sector responses that would be needed to restore and recover the Internet following a disaster.

As the Subcommittee knows, the uninterrupted use of the Internet is a crucial issue for our national and homeland security. The Internet and cyber infrastructure serve as a critical backbone for the exchange of information vital to our economic security. But our analysis has exposed significant weaknesses that could paralyze the economy following massive disruption – regardless of whether this is caused by a terrorist attack or a natural disaster.

Progress has been made over the past decade on technical issues. The Department of Homeland Security, for example, has established a computer security readiness team and is fostering a more sophisticated understanding of cyber risks that could adversely affect the nation's security. However, other issues have not been addressed in government or industry, such as strategic management and governance issues around reconstituting the economy and shoring up market confidence after a wide-scale Internet failure..

Three Gaps in Plans for Restoring the Internet

The Roundtable's report identifies three significant gaps in our nation's response plans to restore the Internet:

- **Inadequate Early Warning System** – First, we found that the U.S. lacks an early warning system to identify potential Internet attacks or determine if the disruptions are spreading rapidly across critical systems.
- **Unclear and Overlapping Responsibilities** – Second, public and private organizations that would oversee restoration and recovery of the Internet have unclear or overlapping responsibilities, resulting in too many institutions with too little interaction and coordination.
- **Insufficient Resources** – Finally, existing organizations and institutions charged with Internet recovery have insufficient resources and support. For example, only a small percentage of the National Cyber Security Division (NCSD)’s funding is targeted for support of cyber recovery.

Collectively, these gaps mean that the U.S. is not sufficiently prepared for a major attack, software incident or natural disaster that would lead to disruption of large parts of the Internet – and our economy. If our nation is hit by a cyber catastrophe that wipes out large parts of the Internet, there is no coordinated, public-private plan in place to restart and restore it. A cyber disaster could have immediate and nationwide consequences to our nation’s security and economy, and we need to be better prepared.

Let me make one other point. Although there is no agreement among experts about the likelihood of a wide-scale cyber disaster, they do agree that the risks and potential outcomes are serious enough to mandate careful planning and preparation.

Recommendations for Government and Business

In my remaining time, let me talk briefly about our recommendations for government and business to improve identification and assessment of cyber disruptions, to coordinate responsibilities for Internet reconstitution, and to make needed investments in institutions with critical roles in Internet recovery.

We believe it is important to understand that response and recovery to a cyber disaster will be different from natural disasters, when the federal government has the leading role. Industry must undertake principal responsibility following an incident for reconstituting the communications infrastructure, including telephone, Internet and broadcast.

We believe that business and government must take action – individually and collectively – to address these issues. Let’s start with government. The Roundtable calls on the federal government to establish clearer roles and responsibilities, fund long-term programs, and ensure that national response plans treat major Internet disruptions as serious national problems. For example, while the Administration says that it has authority to declare a cyber emergency in the National Response Plan -- and will consult with business leaders as part of the declaration, it is not clear how this consultation will occur or what the factors are for declaring an emergency. Nor has Congress clearly authorized the US-Computer Emergency Readiness Team in the Department of Homeland Security to engage in these activities.

Regarding the private sector, our report urges companies to designate a point person for cyber recovery, update their strategic plans to prepare for a widespread Internet outage and the impact on movement of goods and services, and set priorities for restoring Internet service and corporate communications.

But when it comes to protecting our nation – our employees, customers, facilities and communities – the federal government cannot do it alone, and neither can business. The best security solutions will come from a public-private partnership that identifies and acts on ways to improve collaboration. Let me discuss just a few of our recommendations:

- First, since the first 24 hours after a major cyber disruption often determine the overall success of recovery efforts, we must focus more attention on coordinating initial efforts to identify when an Internet attack or disruption is occurring.

- Second, we recommend the creation of a federally-funded panel of experts – from business, government and academia – who would assist in developing plans for restoring Internet services in the event of a massive disruption.
- Finally, we believe that the Department of Homeland Security, together with business, should conduct large-scale cyber emergency exercises, with lessons learned integrated into programs and procedures. These exercises should include senior government and business executives who are fully authorized to act during a cyber emergency and are accountable either to shareholders and boards of directors or, for government, senior political leadership.

Without these changes, our nation will continue to use ad hoc and incomplete tools for managing a critical risk to the Internet – and to our nation’s economy and its security.

Future Business Roundtable Plans

Up to this point I have outlined for the Subcommittee the basis of our observations and our recommendations for government and business to consider. Now I want to spend just a moment telling you about the Business Roundtable’s plans to find solutions to the gaps that we identified.

As an extension of our previous work, the Roundtable will examine coordination processes, protocols and practices across the private sector before, during and after a disruptive event. First, let me say that we are confident that our member companies are able to manage through most disruptions that affect regional, national and global Internet operations. For this reason, the Roundtable will focus its efforts on those large-scale events that no single company is positioned to manage absent widespread cross-industry collaboration in areas such as information sharing and technical support from subject matter experts. We will assess protocols on which institutions respond, but also will look at how early warnings are established as well as how companies access information and service critical disruptions in emergency situations.

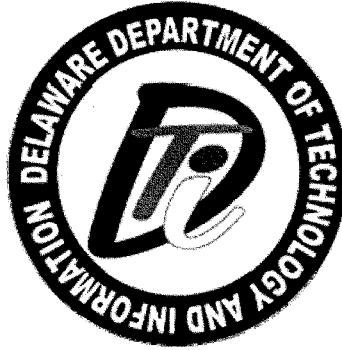
As I noted a moment ago, the Roundtable's review found that there are multiple institutions formally charged with public-private collaboration – with overlapping roles and responsibilities. The Roundtable expects to conduct a rigorous analysis which will depict areas that require consolidation, refinement or creation of new public-private collaboration. We believe this will provide a foundation for meaningful improvements in our nation's ability to protect and restore the necessary Internet infrastructure as well as clarify specific, meaningful and actionable decisions that will lead to well-coordinated response and reconstitution processes.

Conclusion

In conclusion, let me again thank the Chairman and the Subcommittee for the opportunity to present Business Roundtable's report on cyber preparedness and to discuss our recommendations for improvements.

Roundtable CEOs believe strongly that we need a national response to this challenge, not separate business and government responses – and that means better collaboration. Most important, we must start immediately. Because of the widespread consequences of a massive cyber disruption, our nation cannot wait until an incident occurs to start planning the response.

And I assure you that America's CEOs and our companies are committed to do our part.



WRITTEN TESTIMONY OF
THE HONORABLE THOMAS JARRETT
SECRETARY AND CIO, DELAWARE DEPARTMENT OF
TECHNOLOGY AND INFORMATION
and
IMMEDIATE PAST PRESIDENT,
NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION
OFFICERS (NASCIO)

**SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT INFORMATION AND INTERNATIONAL SECURITY
OF THE US SENATE COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENT AFFAIRS**

JULY 28, 2006

As a representative of the Delaware state government and of the National Association of State Chief Information Officers, I appreciate the opportunity to provide written evidence to the US Senate Subcommittee on Federal Financial Management, Government Information and International Security, in relation to the congressional hearing on Internet disruption and plans for resumption. In particular, I would like to provide comments on the ability for a state government to function in today's world without the Internet or without network availability. A massive Internet disruption and prolonged outage is a topic often discussed at the state level, but a lack of policy and of clarity on the roles that the government and the private sector must each play in reconstitution efforts, are major weaknesses.

My testimony is presented from two perspectives. First, representing the great State of Delaware as Secretary of Delaware's Technology and Information (DTI) agency and state Chief Information Officer (CIO), I would like to describe to you some of the critical services provided by the Delaware state government and how these services would be affected in the event of an Internet disruption; and second, as the immediate past President of the National Association of State Chief Information Officers, or "NASCIO," I would like to present perspectives and examples from my fellow State CIOs regarding this important issue. As background, NASCIO represents state chief information officers and information technology executives and managers from the 50 states, six U.S. territories, and the District of Columbia. In most cases, the state CIO is appointed to his or her position by the governor and have executive-level and statewide responsibility for information technology leadership.

As you are likely aware, the Internet and Internet Protocol (IP) based applications have become critical service channels for government at the federal, state and local levels. The Internet is a significant tool that assists almost every department of state government in day-to-day business operations. It is important to understand that a loss of the Internet would not simply mean that fishing licenses could not be purchased online. It would result in substantial interruptions in critical services to citizens, including our most vulnerable citizens. Whether it's the public Internet or a private Internet state network, the convergence of data, voice, video and wireless has changed the way state government conducts business. For state government, the Internet is now a critical part of the fabric of state service delivery, communications and emergency response. Internet no longer only provides just e-government on a state web portal, but has extended to Voice over IP (VoIP) telephony, IP video conferencing and wireless connectivity. . It is an expectation that state government will use Internet availability to transact services, reach out to citizens and support cross-jurisdictional communications.

It is evident that states have become more reliant on the Internet, however Internet dependency has also trickled down to other sectors of government. Many states have moved services to regional offices and local jurisdictions for convenience and cost savings. Delivery of services to constituents, especially in the human services area, is primarily delivered by local governments on behalf of the state and federal government. A lapse or shutdown in Internet availability would disable a vital state-to-local communications mechanism that supports human services, public safety, revenue collections and many other functions that are state administered and locally delivered or simply local programs delivered locally to citizens via the Internet. In addition, there are specific federally related business areas that would be significantly disrupted

by the loss of Internet access, causing increased economic strain, the least of which would be a loss of electronic remittance systems that utilize secure transmissions through the public Internet to keep commerce moving. In times of disasters and emergency response, the Internet is an important channel for intergovernmental communications among local government, regional governments and the state governments. The public relies on government to issue alerts and warnings – systems which are heavily dependent on the IT infrastructure. This dependence on the Internet that exists within all levels of government, demonstrates a real need for intergovernmental collaboration and cooperation, especially during periods of emergency response.

As the State of Delaware's CIO in charge of all state government information and communications technology, one of my highest priorities is maintaining a robust and reliable state network to serve the citizens of Delaware. In Delaware's emergency management arena, we often say that "every incident is local," and this holds true for the states when it comes to major incidents that could threaten access to the Internet or the state's IT infrastructure. The states cannot and should not depend on the federal government for immediate rescue and response in regard to disaster recovery and business continuity.

In the simplest of terms, at the state level, the impact of a loss of Internet and/or the state's network as the result of a major disruption, would be catastrophic. The state and the private sector have a symbiotic relationship in terms of operation and infrastructure and if the Internet were to become unavailable, the state could maintain some services internally, but it certainly would not be business as usual. Without an operating Internet or the state's network, the state would be unable to process most type of financial and other key transactions that support the daily business of government.

Further, without access to our network and the internet, public safety and public health would be put at risk. Our State Police would be unable to process background checks, perform license tag lookups, or seamlessly communicate with their local and federal counterparts. Our Department of Corrections would be on full lock-down, our judicial system would be severely impacted and our ability to provide services through our Department of Youth and Families, like Food Stamp processing and distribution, would become virtually non-existent.

Agencies responsible for providing the funds that keep state government operating, especially in the areas of corporations, franchise and gross receipts taxes would be unable to collect revenue. These three sources alone provide 30% of all Delaware state revenue. Our Health and Social Services and Children's departments, along with Corrections and Homeland Security comprise 39% of our expenditures. Again, without the ability to collect taxes and process payments, vital services for our citizens would not continue.

Disaster recovery at the state level requires intense collaboration and cooperation with key private sector vendors, especially those who provide Internet service; wireless and transparent land services; our 800 MHz digital radio system; and the providers of network security such as firewalls and routers.

Delaware, in concert with our primary telecommunications partner, Verizon, has recently applied for telecommunications service priority (TSP) via the U.S. Department of Homeland Security for all of our main trunk circuits as well as 911 centers and 800 numbers. We currently are awaiting notification of approval. Additionally, we are purchasing wireless priority service from Verizon, which also requires federal DHS approval. Delaware's Technology and Information Agency also purchased several satellite phones to facilitate communication between our data centers in the advent that both wireless and wired alternatives are not readily available.

Delaware state government is increasingly focused on disaster recovery and business continuity efforts and my agency has nearly completed our business continuity plan, which has identified over 500 individual processes that are mission critical. Our disaster recovery (DR) drills have increased in frequency from quarterly to nearly monthly and we held our first ever cyber security tabletop exercise last fall, with our second scheduled for this November. Other agencies, such as our division of public health and agriculture departments are also intently involved in contingency planning targeted at specific threats such as the avian flu.

Obviously, Delaware is not alone in its concerns regarding the potential impacts of a major Internet disruption and the challenges of reconstitution. Through NASCIO, a number of states have contributed their perspective and examples of critical services and applications. These examples clearly illustrate the widespread impact in different domains of government activity.

From the Chief Information Technology Officer, State of Kansas:

The Internet is critical not only for e-government, but also for assisting the state's political leadership in managing natural disasters and other crises. A complicating factor is that the population of the state (2.5+ million) is widely dispersed geographically across 82,277 square miles. The Internet is relied upon to be an adjunct command and control mechanism utilizing an application known as Web Emergency Operations Center or simply WebEOC. Using the Internet, various state agencies access a web portal for the exchange of critical information, whether it be tornados or other severe weather, or a terrorist incident. This also serves as a conduit for information to various Federal government agencies, including FEMA. Hence, an Internet connection is crucial to our crisis management scheme whether it be the Kansas Department of Emergency Management or the National Guard.

From the CIO, Minnesota Department Public Health:

The Internet has become a critical service for public health at the federal, state and local levels. The health and safety of Minnesotans has become more and more dependent on the availability of the Internet. While we have made every effort to implement solutions that do not have a single source of failure, we do have several critical functions that would be seriously, if not dangerously, affected by a disruption to the Internet. Below is a partial list of those services.

1. Inability to use phone service, as Minnesota Department Public Health (MDH) has converted to Voice over IP technology. While MDH has retained a few analog phone

lines, phone service would be greatly reduced and our ability to set up Hot Lines for emergency situations would be difficult at best;

2. Inability to communicate vital health information to local public health departments, the news media and partners using email or Websites. MDH would lose the ability to email partners with critical information regarding outbreaks, hazardous events or public health emergencies. This could be especially damaging during a public health emergency, when accurate, timely information is essential;
3. Inability to connect to the CDC for disease and surveillance activities limiting our ability to respond to outbreaks, hazardous events or public health emergencies. (Examples: TB, Influenza, Polio, West Nile, Food Borne Outbreaks, municipal and private well issues)
4. Inability to notify local public health and health care providers about urgent public health threats. The Internet is the primary method of communication about watching for people with symptoms, providing technical details about case situations, assuring messages to providers and the public are consistent.
5. Inability of the Office of Emergency Preparedness to meet the federal requirement to track available hospital beds. This is an Internet-based system and without the Internet, OEP would spend countless hours calling hospitals and hospitals would spend time tracking this issue rather than providing care;
6. Unable to order vaccines through the CDC. States order from the CDC and they in turn distribute the vaccines around the state. This could be life threatening to citizens if there were any kind of an outbreak.

From the CIO, State of Tennessee

An Internet interruption or intentional disruption could impact state government beyond the obvious reduction of the citizen's ability to receive government service via the Internet. Impact would be seen from those state functions which classically use the Internet or an Internet web site as their interface to government systems. Inspectors or auditors working in the field would not be able to provide information or updates which normally come over the Internet. Examples would include those who monitor such things as crop dusters, or health and human service facilities. At the time when communications and the ability to update data and data bases state wide for situational analysis, determination of statewide trends, or impact would be most vital, it would be cut off. While alternative means of update like phone in or physically going to a terminal in a state office which did not rely on the Internet are available, planning for their use and practice of such alternative methods are not well done.

From the CIO, State of Wisconsin:

The largest potential for network outage may no longer be a physical attack on infrastructure, as the Internet protocols were designed to highly resilient, but rather events like bird flu and pandemics. The projected demands on the Internet during a pandemic flu event could overwhelm capacity to due extreme levels of remote access and stress the public Internet to such a degree that most services could no longer be conducted. There was a recent pandemic simulation in Europe that predicts such an outage.

From the Iowa Department of Public Health:

Approximately 2000 private and public healthcare professionals use the statewide immunization registry over the Internet to ensure children get the right shots at the right time and vaccines are distributed when needed. The Women, Infants and Children (WIC) program providing food assistance to families in need requires Internet access to qualify participants and issue checks. The Health Alert Network uses the Internet to provide information to those responding to a health emergency or bioterrorism alert and to help manage incident as they unfold. The last item may be particularly important. A great deal of the planning for homeland security, bioterrorism, response to natural disasters, and the like at the state level relies on the availability of the Internet.

From the CIO, State of Michigan:

Many critical applications pertaining to State Police, Community Health, Transportation, would be impacted negatively. In many instances the reliance upon technology has replaced any procedure or document that would outline a manual solution and therefore if the Internet were down for any extended period of time, these manual processes would need to be developed causing further delays. The following applications/functions would be inoperable for the Michigan Department of Transportation (MDOT):

- **MiPARS** - Michigan Permitting and Routing System - A substantial portion of this system is web-based. This application would likely be mostly or entirely disabled with a loss of Internet services causing delays or complete inability to issue trucking permits and safe routes to the trucking industry. The impact could be a long delay or inability to provide safe commerce distribution throughout Michigan via the trucking industry.

The following applications/functions would be inoperable for the Michigan Department of Education (MDE). The Michigan Department of Information Technology (DIT) hosts over 40 Internet web based applications for Education and CEPI. The primary customers are the 57 intermediate school districts, 550 public school districts and 4500 schools. One example is State Aid Payments to school districts - portions of this system are web based and used to process \$11 billion in State Aid payments each year.

From the Iowa Department of Public Health:

Approximately 2000 private and public healthcare professionals use the statewide immunization registry over the Internet to ensure children get the right shots at the right time and vaccines are distributed when needed; 2) the Women, Infants and Children (WIC) program providing food assistance to families in need requires Internet access to qualify participants and issue checks and; 3) the Health Alert Network uses the Internet to provide information to those responding to a health emergency or bioterrorism alert and to help manage incident as they unfold. The last item may be particularly important. A great deal of the planning for homeland security,

bioterrorism, response to natural disasters, and the like at the state level relies on the availability of the Internet.

From the CIO, State of Georgia:

A major concern from Georgia is the recognition that some local government agencies use the internet to connect to state services. A particular concern is local law enforcement access to the FBI's National Crime Information Center (NCIC). Some of the local agencies have migrated their access to the internet with no backup connectivity. The loss of the internet has the potential to put lives at risk by denying officers in the field access to NCIC criminal information.

An extended internet disruption could cause major issues since many agencies have probably leveraged the internet without even knowing it through services offerings. Also, constituent to state communications over the internet is becoming more and more core to supporting our constituents. During Katrina, several agencies within Georgia were using the internet to gather data, disseminate data and otherwise manage the influx of people and supporting their varied needs. The Department of Education was communicating with the other states to share student information in a secure but timely manner. The law enforcement community was sharing information about displaced parolees, etc. The Department of Human Resources was communicating with its peer agencies and the federal government about medical needs.

The many illustrations from my state colleagues represent only the tip of the iceberg of state services and applications that would be severely impacted as a result a major Internet disruption. Yet with all of our individual focus on the provision of services to our citizens and the continuity of government, it is apparent that still is an overwhelming need for increased collaboration within state government, with local governments, between neighboring states and with the federal government. Although states have prepared themselves though redundant provisioning, private backbone networks and business continuity planning, the impact would still be severe.

The lack of a national policy, direction and clarity for Internet resumption will not serve the needs of citizens during a crisis. There is no apparent protocol or process for communication between entities in the advent of an orchestrated large scale denial of service cyber attack or major disaster which would disrupt Internet availability. There needs to be a clear and concise communication system within and throughout all levels of government *and with critical private sector entities such as telecommunication carriers, internet service providers, financial institutions and major it vendors*. NASCIO urges action to determine the appropriate roles and responsibilities of the federal government, state government and the private sector. As the CIO for the State of Delaware and as the Immediate Past President of NASCIO, I appreciate the work of the Subcommittee in addressing this national challenge. NASCIO stands ready to contribute in a meaningful way as needed.

Questions for the Record
Senate Homeland Security and Governmental Affairs
Federal Financial Management, Government Information, and International Security Subcommittee
"Cyber Security: Recovery and Reconstitution of Critical Networks"
July 28, 2006
Under Secretary George Foresman

Questions from Senator Tom Coburn

1. You testify: "as the Department matures we are preparing for large scale cyber disasters. Our strategic intentions are ambitious and will require resolution of multiple impediments, such as:

- Identifying incidents and providing early warning;
- Deploying Federal assets and services more efficiently to mitigate damages where disruptions occur;
- Responding to the speed of attacks and disruptions, which will require new technologies and skill sets in our workforce; and
- Maximizing the use of tools that promote and integrate privacy protections as well as real-time security needs."

You conclude in your testimony that "Our progress to date is tangible: we have a construct for public-private partnership; we have a track record of success in our cyber operations; we have established relationships at various levels to manage cyber incidents; we have built international communities of interest to address a global problem; and we have tested ourselves at a critical development stage and will continue to examine our internal policies, procedures, and communications paths in future exercises."

- How do your tangible successes square with the impediments you have outlined? How have your successes moved the Department closer to fixing the impediments? How much money and what projects are underway to mitigate the impediments?

Response: The budget for the National Cyber Security Division for FY06 is \$92.4 million, and these funds are leveraged across a range of strategic and operational programs that enhance our overall state of cyber preparedness and specifically help to overcome the impediments identified above. While much remains to be done, the Department has made significant advances in each of the noted areas:

- We have implemented programs such as the Internet Health Service, Project EINSTEIN, and others that substantially augment our capabilities in incident handling and watch and warning to enable us to respond commensurately to the increasing speed and sophistication of cyber attacks.
- We are actively leveraging our relationships with all of our partners, including the expertise and capabilities of Federal agencies.
- Developing new technologies and enhanced skill sets that will enable us to respond with greater speed must be a steady-state activity: as our adversaries improve the speed and efficiency of their tools, we must constantly be doing so as well. That effort will require a long-term commitment and sophisticated approaches; however, each of our initiatives presently underway contributes significant incremental improvements in our speed and effectiveness.
- Finally, as we develop the programs and initiatives that move us toward these strategic objectives, we are consciously and deliberately incorporating into them processes and mechanisms to protect individuals' privacy while maintaining the ability to monitor conditions and respond as necessary in real-time.

Questions for the Record
Senate Homeland Security and Governmental Affairs
Federal Financial Management, Government Information, and International Security Subcommittee
"Cyber Security: Recovery and Reconstitution of Critical Networks"
July 28, 2006
Under Secretary George Foreman

The discussion that follows describes more fully the specific programmatic successes in each of these areas and the manner in which they help to mitigate the corresponding impediments.

Impediment 1: Identifying incidents and providing early warning.

Successes: The early identification and attribution of hostile intent in cyber activity, and effectively providing timely alerts and warning of it to those who may be impacted, present serious challenges that require a sophisticated and focused strategy to resolve. Cyber attacks can be executed and spread at great speeds, and do not respect global boundaries or conventional defenses. Indeed, even when anomalous activity is observed, experts struggle to identify whether it is hostile or non-malicious. The U.S. Computer Emergency Readiness Team (US-CERT) has implemented a number of programs that specifically address these challenges by (1) broadening our real-time situational awareness of activity as it is unfolding; (2) strengthening our analytical capacity to discern and distinguish between hostile and non-malicious activity; and (3) improving our information sharing channels with key communities to ensure more rapid exchange of reciprocal alert and warning information when anomalous and potentially malicious activity is observed.

Broadening Situational Awareness. Two programs that best illustrate successful US-CERT efforts to expand the Department's situational awareness of cyber events to support more rapid identification and warning of hostile activity are the Internet Health Service and the EINSTEIN program.

The Internet Health Service (IHS) is a web-based suite of commercially available Internet and security monitoring products that US-CERT makes available through its secure portal to members of the Federal Government Forum of Incident Response and Security Teams (GFIRST). By offering this suite of tools, US-CERT enables Federal and State government agencies to augment their own network monitoring capabilities, which expands their individual situational awareness. By promoting information sharing between US-CERT and the participating GFIRST agencies, it also expands US-CERT's situational awareness more broadly across the electronic landscape, allowing for the spotting of trends and early analysis of cyber activity across the public and private sectors – in real time.

Similarly, while the IHS facilitates the ability of participating agencies to monitor their own network status, US-CERT's EINSTEIN Program enables US-CERT directly to monitor network activity across participating Federal departments and agencies. At present, seven Federal departments or agencies participate in the program with an additional agency expected to join in the near future. This capability has demonstrated its value through the early identification of compromised systems.

Strengthening Analytical Capacity. US-CERT is working with the private sector to identify the criticality of vulnerabilities and coordinating with the vendors and the information technology community to provide timely and actionable information to the Federal agencies,

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foreman

the critical infrastructure sectors, and to the general public about steps they can take to protect themselves. The recent analysis and communications efforts regarding Microsoft vulnerability MS06-040 provide an illustrative example of successful vulnerability management and incident response.

Improving Information Sharing. Finally, US-CERT is facilitating more effective and timely exchange of reciprocal alert and warning information by improving information sharing channels and conduits among all of our partners. One such success, the US-CERT Secure Portal, has already been mentioned above. The Portal, which operates as a component of the Homeland Security Information Network (HSIN), was established to serve as a secure environment for collaboration and information sharing among government, industry, and the Information Sharing and Analysis Centers (ISACs). It is presently available to over 2,000 participants and provides them access to collaboration features to include secure messaging, libraries, forum discussions, alerts, chat rooms, task tracking, and a user locator, among other features.

NCSD/US-CERT is also moving ahead aggressively with our international partners on coordination of response to cyber-based attacks. Specifically, we are engaged in discussions with Australia, Canada, New Zealand, and the United Kingdom to streamline the sharing of threat, vulnerability, and incident information to resolve fast-spreading attacks.

Finally, we are leveraging our exercise experience to guide improvements in our management of global cyber threats and attacks. The national cyber exercise, *Cyber Storm*, conducted in February 2006, was successful in examining the communications among public and private sector organizations in the context of a response to a cyber attack. To formalize lessons learned from *Cyber Storm*, US-CERT is developing a Private Sector Concept of Operations (CONOPs) to delineate information sharing activities and coordination efforts with the private sector for cyber incidents. US-CERT has received input from the Information Technology Information Sharing and Analysis Center (IT-ISAC) and will work with other stakeholders to gather and baseline roles and expectations.

Impediment 2: Deploying Federal assets and services more efficiently to mitigate damages where disruptions occur.

Successes: The Department has also made demonstrable progress in planning for the deployment and use of Federal resources to assist in the coordination of response to a disaster or emergency with a cyber dimension. The establishment of the Cyber Incident Annex in the National Response Plan represents a significant achievement and one that recognizes the unique nature of a cyber incident. Specifically, given the distributed nature of the Internet and the significant role of the private sector in its operations, a cyber incident may or may not require the deployment of Federal assets and services.

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

As we review the Cyber Annex for the development of an Operations Plan, we are considering the range of needs for response and recovery efforts that will require advance planning and articulation. This will include consideration of potential legal and policy issues surrounding the provision of Federal assets and services, as well as the management of private sector donated resources such as envisioned in the NET Guard provision of the Homeland Security Act. The Cyber Incident Annex Operations Plan will provide for preparedness, response, and recovery support, and incorporate appropriate coordination with Emergency Support Function 2 – Communications (ESF-2), for which a separate Operations Plan was recently adopted.

Impediment 3: Responding to the speed of attacks and disruptions, which will require new technologies and skill sets in our workforce.

Successes: As indicated above, the speed of cyber attacks and disruptions presents a challenge to our incident response efforts. The successes of US-CERT Operations in incident and vulnerability handling discussed above demonstrate progress in developing new skill sets and technical tools and capabilities to support more effective incident response.

The work of NCSD's Strategic Initiatives Branch addresses both research & development and workforce and training issues. For example, NCSD works directly with the White House Office of Science and Technology Policy to co-chair the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), which developed and published the *Federal Plan for Cyber Security and Information Assurance Research and Development*. This document articulates Federal needs for cyber security research and development specifically to meet new technology needs. To strengthen the skill sets of our workforce, the Cyber Security Training and Education Program provides resources and performs activities to meet the training, education, and certification needs of IT security professionals within the Federal government and private industry. By focusing resources on improved cyber security education for IT professionals, increasing the efficiency of existing cyber security training programs, and promoting widely recognized, vendor-neutral cyber security certifications, NCSD is actively working to improve the Nation's pool of educated cyber security professionals.

Impediment 4: Maximizing the use of tools that promote and integrate privacy protections as well as real-time security needs.

Successes: With the protection of information systems, protecting the privacy and integrity of personal and institutional information and data represents one of the cornerstone objectives of cyber security policy. Privacy and security are inextricably linked, and as we implement new security measures to help to achieve these objectives, we are also mindful that our methods and tools do not themselves intrude upon these interests.

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

In implementing its policies and programs, including those discussed above, NCSD and US-CERT work closely with the DHS Privacy Office to ensure that our activities properly safeguard privacy interests. The US-CERT EINSTEIN Program represents a good example of this integration of privacy protections into a programmatic tool to support real-time security needs. As discussed above, EINSTEIN is a robust technology deployed by DHS in cooperation with participating Federal agencies that enables US-CERT to track attacks against agency networks. Given its powerful use of near real-time information, the program underwent a complete privacy impact assessment (PIA) to ensure strict adherence to Federal privacy laws.

- How does the internet disruption working group fit into correcting the impediments you outline? What actionable results have come out of this group? Do their duties overlap with other DHS organizations?

Response: The Internet Disruption Working Group (IDWG) is a strategic partnership between NCSD and the Office of the Manager of the National Communications System (OMNCS). It provides a forum to address security concerns surrounding the growing dependency of critical infrastructures and national security and emergency preparedness (NS/EP) users on the Internet for communications, operational functions, and essential services. The membership of the IDWG consists of representatives from Internet backbone providers and security experts from government, private sector, academia, and international organizations. The goal of the IDWG is to promote resiliency of the Internet, which it does by examining risks; improving preparedness, situational awareness, and information sharing; and identifying measures that need to be taken to protect against nationally significant Internet disruptions. The IDWG's activities do not overlap with those of other DHS organizations or programs. Rather, the IDWG leverages the contributions of other components and adds value to the efforts of others through its findings and recommendations.

In June 2006, the IDWG hosted its first tabletop exercise (TTX) to discuss industry and government roles and responsibilities in the event of an Internet disruption. The exercise included discussion regarding improving incident identification techniques and early warning practices currently used by both government and the private sector. The IDWG TTX included participation from 35 subject matter experts from the public and private sector. The TTX generated productive discussion among the participants concerning the analysis of anomalous Internet activity and information sharing to identify the malicious nature of an unfolding cyber event early in its onset to take appropriate actions (warning and other responsive measures) that will prevent it from developing into a cyber Incident of National Significance (CINS). Collaborating with our private sector stakeholders and identifying current gaps will enable prioritization of programmatic activities and further mitigate this impediment.

One key finding that emerged from the June IDWG TTX was the need for an institutionalized, networked sharing environment that builds on existing collaborative efforts and individual working relationships. Accordingly, the IDWG is undertaking an Information Sharing

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

Assessment to understand better the information sharing landscape involving Internet incidents. It will document the interactions between and among different levels of government and private industry, as well as other relevant organizations, such as academic institutions, in order to identify incident reporting success factors and improve both the flow and the value of threat, vulnerability, and incident reports. It will also assist DHS in identifying gaps in current practices in order to formulate recommendations for future action. The assessment will yield recommendations for leveraging current information sharing relationships, including informal sharing mechanisms, in a systematic way to increase situational awareness. The IDWG Information Sharing Assessment will be completed in the first quarter of FY07 and the Internet community will be briefed on its findings at the next IDWG Forum. The report is expected to include estimates of the resources required and a timeline for actions needed to implement the recommendations.

As partners in the IDWG, the OMNCS and NCSD are also planning to collaborate with stakeholders on a response and recovery focus team that will explore the question of Federal asset and service deployment during a CINS, another impediment referenced in the testimony. The IDWG also realizes that the increasing reliance on next generation networks and the degree to which there is convergence of cyber and telecommunications is increasing the complexity of the network and decreasing the time given to respond to attacks. Through the public/private partnership of the IDWG, government and industry are facilitating solutions to address this heightened risk by identifying areas for further research and development in new technologies.

- Does the Internet Disruption Working Group have authority to examine layer 1-3 of the internet? Does it have authority over SS7? What capabilities does it have to examine the core transportation layers of the internet?

Response: Because the infrastructure that supports the Internet is owned and operated by the private sector, the government must work with these entities as a partner to inspect, or conduct research on, layers 1-3 of the Internet. DHS is actively working with the private sector to increase collaboration and information sharing to support further research efforts examining layers 1-3 of the Internet. The existing relationships that NCSD and OMNCS enjoy with private industry through the National Coordinating Center for Telecommunications, US-CERT, the IT-ISAC, and the IT and Communications Sector Coordinating Councils (SCCs), greatly assist in this effort.

The IDWG draws upon the Department's authorities under statute and executive orders and directives to conduct its activities in support of preparedness, response, and recovery missions. It provides a venue for Internet experts to share their existing knowledge and findings, and to make recommendations about areas requiring further research.

Signaling System 7 (SS7) is a network protocol used on the out-of-band network supporting the Public Switched Telephone Network (PSTN). Standards organizations such as the International Telecommunication Union - Telecommunication Standardization Sector (ITU-TSS) and

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

American National Standards Institute (ANSI) add specifications to this protocol, as necessary, to advance its functionality. As a telecommunications function, the SS7 network is subject to provisions of the Communications Act of 1934, as amended, oversight of which is vested in the Federal Communications Commission (FCC).

- CWIN, HSIN, US CERT Alerts are all internet based. What backup plans do you have to send actionable information out in the event of an incident of national significance? By placing all of these resources on-line do you believe the internet will not go down?

Response: DHS utilizes the Internet for communications through HSIN, the US-CERT Portal, and for the National Cyber Alert System to deliver messages to the public and critical infrastructure operators. The Internet is designed to be a resilient network that recovers from outages and other disruptions. While we believe that it is unlikely that the Internet would go down in its entirety, there is a possibility that a major disruption could hinder vital communications. Recognizing this potential, DHS also leverages backup systems and analog communications channels for information sharing and dissemination.

Sound risk management practices demand redundancy and diversity in systems supporting critical needs. Accordingly, we do not rely exclusively on any one type of technology or communications means for critical information dissemination needs. In the event of a catastrophic Internet disruption, DHS would rely on private and government networks and additional channels that do not rely upon the Internet to send actionable information to the public and critical infrastructure operators.

CWIN provides an example of how system redundancy can provide communications in the event of network outages. CWIN is a survivable network that does not utilize the public switch network. In the event that the internet goes down, CWIN can ensure that voice and data communication capabilities will still exist between Federal agencies, State and local governments, and the private sector.

2. In your testimony you suggest we must prevent cyber incidents of national significance. I agree that that effort is vital. However, is it possible for our critical infrastructures to get to zero successful penetrations? If not, should we be focusing more attention and resources on to decreasing our recovery time and reconstitution time?

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

Response: While we endeavor to minimize successful penetrations on our critical infrastructure, and zero would be optimal, we are not likely ever to be completely risk free. We are focusing attention and resources on addressing cyber incidents of national significance, including preparation for, response to, and recovery from such incidents. These efforts include seeking to prevent penetrations to the best extent possible, but it is important to focus on risk management efforts that determine priority protective measures that not only address prevention, but also enable effective recovery and reconstitution from incidents that occur in spite of our prevention efforts.

The DHS focus on Internet recovery and reconstitution consists of three primary elements that receive a significant portion of NCSD's resources: (1) US-CERT Operations, with its incident handling, vulnerability management, and communication and coordination responsibilities; (2) the IDWG, with its mission to address Internet disruption as one of our key cyber risk management efforts; and (3) the National Cyber Response Coordination Group (NCRCG), the principal Federal interagency mechanism delineated in the National Response Plan for preparing for and responding to cyber incidents of national significance.

3. Why, almost a year after announcing the creation of an Assistant Secretary for Cyber Security and Telecommunications is the position still vacant? What has prevented DHS from filling this position? How will the new Assistant Secretary for Cyber Security and Telecommunications have the power to effectively resolve the difficulties the National Cyber Security Division has been grappling with, including organizational stability; hiring and contracting issues; establishing effective partnerships with federal, state, and local governments and the private sector; and achieving two-way information sharing with these stakeholders? You point out that the new Assistant Secretary needs to be the right combination of skill, experience and leadership to succeed; however, you do not mention the need for authority, mission clarity or priorities. Do you have a guiding document that defines these important strategic concepts?

Response: The Department is pleased to announce that on October 11, 2006, Mr. Gregory Garcia was sworn in as Assistant Secretary for Cyber Security and Communications by Secretary Michael Chertoff. Mr. Garcia joins the Department from the Information Technology Association of America, where he was Vice President for Information Security Policy and Programs. In that capacity, he led the public debate on cyber security policy and national cyber readiness. His contributions and experience in the cyber telecommunications field in both the public and private sectors are expected to enhance continuing progress in this area.

Mr. Garcia has worked closely with the Department over the past few years in his role on the IT Sector Coordinating Council and with industry to create the National Cyber Security Partnership. He helped to draft and enact the Cyber Security Research and Development Act of 2002 during his tenure with the U.S. House of Representatives Committee on Science. He has also worked to strengthen encryption control regulations while with the Americans for Computer Privacy and he was active on international trade and IT policy at the Americans Electronics Association.

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

DHS's operating authorities with respect to the cyber security and disaster and emergency assistance missions are grounded in the Homeland Security Act of 2002, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, and executive directives and orders including, but not limited to Homeland Security Presidential Directives (HSPDs) 5 and 7 and Executive Orders 12472 and 12656, as amended. These authorities are further developed in guidance set forth in policy documents including the National Strategy for Homeland Security, the National Strategy to Secure Cyberspace, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the National Response Plan, and the National Infrastructure Protection Plan (NIPP). Collectively, these documents provide the guidance for DHS's cyber security priorities, which include leading a cyber risk management program, and building and enhancing the National Cyberspace Response System.

4. DHS recently released the National Infrastructure Protection Plan. Its success hinges on information sharing between the federal government and the private sector. However, recent incidents indicate that the government has trouble protecting sensitive information. The government also does not have a good record of sharing sensitive intelligence-derived threat data with the private sector. What benefit is there to the private sector to cooperating with DHS in Internet Recovery planning? Why is the private sector being asked to shoulder the burden of Internet Recovery planning?

Response: DHS recognizes the private sector's concerns regarding information sharing and has taken several steps to address those concerns, including implementing improvements to the Protected Critical Infrastructure Information (PCII) Program; building trusted relationships with private sector entities through productive, collaborative efforts on incident response; establishing a historic partnership for strategic and operational information sharing and collaboration in the NIPP; and holding classified briefings with cleared private sector representatives. We understand the importance of mutually beneficial trust relationships and are working to enhance reciprocal information sharing efforts that provide value to our stakeholders.

Because the private sector owns and operates virtually all of the infrastructure that supports the functioning of the Internet, Internet recovery planning, like other aspects of cyber security, cannot be accomplished by government acting alone. However, neither can the private sector on its own effectively address planning needs across the full geographic, economic, and social landscape that the Internet serves. Therefore, Internet recovery planning, like critical infrastructure protection, generally, is a shared responsibility that requires a shared effort by government and the private sector working in collaboration. In general, it is a part of private sector operational prerogative to make the decisions and take the actions necessary and prudent to enhance the resilience of their systems and ensure their continuity of operations. Such decisions and actions include appropriate recovery planning and other preparedness activities. However, the private sector can benefit from cooperation with DHS; as a coordinating body for planning, DHS will also serve as a coordinating body for response to an incident. Such

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

coordination helps to minimize confusion and replaces actions taken in isolation with a concerted effort that leverages the collective expertise and capabilities of all parties to address the collective problem.

We appreciate the increasing willingness of the private sector to engage in collaborative planning efforts that benefit the greater community of infrastructure owners and operators and our economy as a whole, and we will endeavor to maintain and enhance the mutually beneficial aspects of this public-private partnership.

5. Why is the government's role different in buttressing the defense of cyberspace, on which our nation and economy increasingly rely, than say our national air defense capabilities?

Response: Unlike the resources for national air defense, which are government-owned, the private sector owns and operates virtually all of the infrastructure that supports the functioning of the Internet. As noted in the immediately preceding response, this fact automatically changes the paradigm with respect to the government's role as compared to the national air defense example. As provided for by the National Strategy to Secure Cyberspace and HSPD 7, NCSD serves as a national focal point for addressing cyber security. NCSD's mission is to collaborate with public, private, and international entities to secure cyberspace and America's cyber assets. Collaboration and partnership are key elements for the defense of cyberspace, and the government as a coordinating body is a critical component of that mission.

6. NCS and NCSD have overlapping responsibilities related to Internet recovery. Why is there no formal breakdown of responsibilities between the two organizations? What improvements could DHS make to the organizational structures of NCS and NCSD?

Response: The responsibilities of OMNCS and NCSD related to Internet recovery are complementary, and reflect both the distinctions between and convergence of the IT and Telecommunications Sectors. As currently articulated in the NRP, a clear role is delineated for NCS in the context of ESF-2 and a clear role is defined for NCSD in the context of support for ESF-2 as well as for the Cyber Incident Annex. NCS has recently revised the Operations Plan in support of ESF-2, and NCSD/US-CERT as Executive Agent for the NCRCG is developing an Operations Plan for the Cyber Incident Annex.

OMNCS and NCSD collaborate on a regular basis to ensure that issues related to Internet recovery are addressed jointly and that each organization's expertise is brought to bear. This collaboration is reflected in our current initiatives to address Internet recovery as well as other ongoing activities and include coordination in the NIPP, joint leadership of the IDWG, and operational cooperation. Additionally, in August 2006, OMNCS and NCSD leadership engaged in a strategic planning session to further define the interaction between these organizations as they operate as an integrated Office of Cyber Security and Telecommunications (CS&T). Deputy Under Secretary for Preparedness, Robert Zitz, convened this meeting to engender the development and refinement of the CS&T vision and strategic plan.

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

As detailed in the NIPP, DHS is the Sector Specific Agency (SSA) responsible for both the Information Technology (IT) Sector and the Telecommunications Sector. The Department also provides expertise and guidance to other sectors regarding the cyber elements of their infrastructure. The NCSD works closely with the IT Sector Coordinating Council (IT SCC), which was formally launched in January of this year. Similarly, OMNCS works closely with the Communications SCC. NCSD and OMNCS are working together and with the respective SCCs to coordinate on the development of the Sector Specific Plan (SSP) for each sector to reflect convergence, leverage expertise, and ensure complementary programs. (This point is discussed more fully in the response to Q04081 below.)

The operational components of the OMNCS and NCSD – the NCC and the US-CERT, respectively – are also enhancing their working relationship for response and recovery initiatives. The US-CERT Watch and the NCC coordinate on a daily basis, and they will soon be co-located to further that collaboration. NCSD and OMNCS are also collaborating on a number of other initiatives (including the IDWG as discussed above), and NCSD works closely with OMNCS on preparing for recovery of critical communications networks and services in its role as a supporting agency under the NRP for ESF-2 (Communications), which NCS leads. This is a critical component of advanced planning and ensuring coordinated recovery efforts.

7. How is DHS ensuring that plans for recovery, such as the National Response Plan and the National Infrastructure Protection Plan are completed and widely distributed and utilized?

Response: NCSD worked closely with the NIPP Program Management Office (PMO) on the development of the NIPP Base Plan. The NIPP Base Plan went through two rounds of public review with over 5000 of the Department's Federal, State, local, and private sector security partners providing comments. The final version was released on June 30, 2006. The plan provides the unifying structure for protecting our Nation's critical infrastructure and key resources (CI/KR) by using a risk management framework for combining consequence, vulnerability and threat information to produce a comprehensive, systematic national risk assessment.

To supplement the NIPP Base Plan, each SSA is working with its Federal, State, local, and private sector partners to develop an SSP for its sector. These SSPs will detail the particular application of the risk management framework to each of the 17 CI/KR sectors and complement the NIPP Base Plan.

To ensure wide distribution of the NIPP, the NIPP PMO and the DHS Office of Public Affairs implemented a comprehensive rollout strategy to announce the release of the plan. We anticipate that the SCCs and Government Coordinating Councils (GCCs) will continue to seek opportunities to provide information on DHS infrastructure protection initiatives and invite greater participation in the process to develop and implement the SSPs.

Questions for the Record
Senate Homeland Security and Governmental Affairs
Federal Financial Management, Government Information, and International Security Subcommittee
"Cyber Security: Recovery and Reconstitution of Critical Networks"
July 28, 2006
Under Secretary George Foresman

With regard to the NRP, the Homeland Security Council directed DHS to complete an interagency review of the NRP to incorporate critical revisions prior to the onset of the 2006 hurricane season. The revisions were based on organizational changes within DHS, as well as the lessons learned from the experience of responding to hurricanes Katrina, Wilma, and Rita in 2005. Incident to this process, as noted above, NCS, as lead agency for ESF-2, Communications, completed a comprehensive rewrite of the ESF-2 Operations Plan, which included an effort by all support agencies to develop or revise agency Standard Operating Procedures in support of the Operations Plan. The NRP Notice of Change precedes the first official interagency review of the NRP, and DHS intends to initiate a comprehensive stakeholder review of the NRP in the fall of 2006.

8. Please provide a concrete example of a threshold at which a disruption of the Internet would trigger the National Response Plan and what the federal government would do in this situation.

Response: DHS uses standardized and reliable methods to assess the criticality or severity of a new or emerging cyber security event. The DHS US-CERT CONOPs includes a matrix of factors that are weighed in determining the 'severity' of a security event. Certainly a complete failure of the Internet would constitute a major disruption that would trigger the National Response Plan (NRP). However, there are any number of other disruptions that could rise to the level of a incident of National significance activating the NRP and the Cyber Incident Annex to the NRP. For example, a directed attack against the Domain Name System or core routing protocols such as the Border Gateway Protocol, both of which are essential to making the Internet function properly, would constitute an incident of National significance.

9. Is the private sector reluctant to share information with DHS because they do not perceive DHS to have a clear role in reconstitution?

Response: Members of the private sector, in various forms and forums, have articulated their individual and collective concerns about sharing information with DHS, and these concerns include uncertainty about the government's role in Internet reconstitution. Therefore, we have initiated a process with our private sector partners to develop a response plan for Internet recovery and reconstitution that will, among other things, clearly delineate the respective roles and responsibilities for industry and government in the event of a major Internet disruption. Activities such as the IDWG TTX have been held to strengthen the public/private relationship and to bring more clarity to the question of government and private sector roles and responsibilities.

More broadly, the Department, as part of its overall responsibility to lead infrastructure protection efforts, has taken actions designed to clarify roles and responsibilities and strengthen the environment of trust necessary for robust information sharing. These actions include the delineation of the Sector Partnership Model under the NIPP, which formalizes the collaboration framework between government and industry through the SCCs and GCCs. As previously

Questions for the Record
Senate Homeland Security and Governmental Affairs
Federal Financial Management, Government Information, and International Security Subcommittee
"Cyber Security: Recovery and Reconstitution of Critical Networks"
July 28, 2006
Under Secretary George Foresman

stated, DHS serves as the SSA responsible for both the IT and Communications Sectors, and assists other sectors with the cyber elements of their infrastructure.

An additional example of success in this area is the partnership between the telecommunications industry and the NCS, in which there is a long-standing arrangement to respond to communications disasters and emergency with close sharing of information, resources, expertise, etc., for the good of the industry and government alike. The NCS and industry trust arrangement is a model that is being leveraged throughout the Preparedness Directorate.

DHS has also undertaken specific programs, such as the Protected Critical Infrastructure Information (PCII) to address private sector concerns in this regard. DHS has recently made improvements to PCII and other information sharing mechanisms to address those concerns.

10. What investments, if any, has DHS made in communications capabilities that enable the nation to coordinate software fixes in the event that key networks functions were lost? Is there unused spectrum that could be utilized to allow vendors to push fixes to federal agencies and critical infrastructure facilities in a time of crisis?

Response: The National Telecommunications and Information Administration (NTIA) of the Department of Commerce, and the Federal Communications Commission (FCC) have responsibility for the allocation and assignment of radio frequency spectrum for government, public safety, and commercial uses. During the response to hurricane Katrina, these agencies worked closely with the NCS under the auspices of ESF-2 to provide spectrum assignments for emergency use. In a major cyber event these processes could also be employed as appropriate and necessary to provide spectrum for emergency response needs.

Additionally, today the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs of the NCS provide priority voice and voice-grade data connections through the public-switched telephone network that could be used, if needed, for disseminating critical software patches necessary to deal with cyber events. In the future, this priority capability will be available at much higher rates of speed, in the IP space as a result of NCS investments in national and international standards for priority handling of government and other critical users' communications in the next generation networks.

11. A number of reports have suggested that DHS should create a cross-sector public-private center/capability to incident response, including nationally significant cyber incidents. Some have suggested that this model could be based on the National Coordinating Center for Telecommunications? Does DHS have plans to create an incident response center? If one already exists, does it pass any information or actual information beyond "port activity" to the private sector? Is this information actionable?

Response: DHS has established the National Infrastructure Coordinating Center (NICC), which is a 24x7 operations center and an element of the National Operations Center (NOC). The

Questions for the Record

Senate Homeland Security and Governmental Affairs
Federal Financial Management, Government Information, and International Security Subcommittee
"Cyber Security: Recovery and Reconstitution of Critical Networks"

July 28, 2006

Under Secretary George Foresman

primary mission of the NICC is to maintain situational awareness of the Nation's CI/KR and provide a conduit for information sharing and coordination between and among government, critical infrastructure owners and operators, and other industry partners – including SCCs, GCCs, and ISACs. In support of its mission, the NICC is responsible for disseminating a wide range of DHS products containing warning, threat, and critical infrastructure protection information to the private sector and government entities. The NICC also receives situational and operational information from the private sector and disseminates that information throughout the NOC and, as appropriate, to other government operation centers and industry partners.

In direct collaboration with the NCC and the US-CERT, the NICC can act as an additional information sharing mechanism to support the dissemination of cyber-specific information to the private sector. Using the Homeland Security Information Network – Critical Sector (HSIN-CS) the NICC is positioned to assist making DHS cyber products available to a broad population of the Nation's CI/KR owners and operators.

12. In 2004, Senator Bennett championed an amendment to the Defense Production Act (DPA) that affirmatively stated that the federal government could use DPA to assist the private sector prepare for, respond to, or recover from failure. What steps has DHS taken to ensure that these authorities could be tapped to support the Cyber sector in recovering Internet functions critical to national defense and economic security?

Response: Under the Defense Production Act (DPA), the Federal government, acting through delegated authority to DHS/FEMA, may provide certain contract priorities to the private sector CI/KR entities to obtain scarce resources necessary in an extraordinary disaster event. Congress recognized this private sector need when it specifically broadened the scope of the DPA and added "critical infrastructure protection and restoration" to the definition of "national defense" in the Defense Production Act in 2003.

Under Title I, the DPA can be used to protect or restore critical infrastructures by: (1) requiring priority performance of contracts or orders (other than contracts of employment); and (2) making allocations of materials, services, and facilities to promote national defense. Under Title III, the Act can be used to provide financial incentives for critical infrastructures to ensure the availability of materials, services and technologies. For example, Title III can be used to establish, maintain, modernize, or expand domestic production capacity for essential technology items, components, and industrial resources, for which a viable capacity does not exist or is insufficient to meet demand. Under the NIPP framework, DHS is working with its partners to explore ways in which these tools can most effectively be applied to support the needs of CI/KR entities in the context of the response to a disaster or emergency. We expect this process will yield guidance on general framework principles that will then be tailored to the particular requirements that individual sectors are likely to confront in specific circumstances such as a major disruption of Internet function.

Questions for the Record
Senate Homeland Security and Governmental Affairs
Federal Financial Management, Government Information, and International Security Subcommittee
"Cyber Security: Recovery and Reconstitution of Critical Networks"
July 28, 2006
Under Secretary George Foresman

13. In February of this year the UK accused China of purposely attacking its systems. If U.S. agencies were under a sustained attack from foreign powers or transnational groups, what would your agency's response be? How would such a response be coordinated across agencies and in the EOP?

Response: NCSD would be pleased to offer a classified briefing on this topic.

Questions from Senator Tom Carper

1. NCSD appears to execute significant incident response capabilities on behalf of OMB and is also tasked with managing the overall national cyber incident response functions. Given the limited resources at DHS, how would the department prioritize support in a crisis? Would federal agencies get priority for recovery support or would national infrastructures get priority support?

Response: NCSD's responsibilities do not require NCSD to choose between providing support to Federal clients or assisting private sector CI/KR entities in the context of the response to a cyber Incident of National Significance. On the contrary, the response framework under the NRP is designed to ensure that both of these interests receive equally robust support.

Under the NRP Cyber Incident Annex, US-CERT as Executive Agent for the NCRCG –assists in coordinating response capabilities of the Federal government. In addition, NCSD through US-CERT also works with State and local government authorities and critical private sector entities to facilitate information sharing in support of broad situation awareness and coordination of concerted responsive measures by all parties. Finally, NCSD provides indications and warnings of potential threats, incidents and attacks; analysis of cyber vulnerabilities, exploits, and attack methodologies; technical assistance; and forensic analysis which aids in investigation, attribution, defense against the attack, and where appropriate and possible, prosecution of the perpetrator.

Moreover, it is equally important to recognize that in response to a CINS that threatens Federal communications and information systems, the resources of the NCSD would be augmented substantially by the parallel role that the National Communications System (NCS) would also be performing. Under Executive Order 12472, the NCS is the primary body charged with ensuring the reliability, resiliency, response, and recovery of Federal systems used for national security and emergency preparedness communications. The NRP reflects this mission by assigning NCS as the primary agency to act as coordinator for ESF #2 (Communications). In this role, NCS, like NCSD, can leverage and marshal the capabilities and resources of its supporting agencies to contribute to addressing the response and recovery needs of Federal NS/EP users.

2. DHS has developed and tested Einstein technology. Why, if this technology obviously works and you have the resources to deploy it, why hasn't your own Department deployed it. In other words why isn't DHS leading by example?

Questions for the Record

Senate Homeland Security and Governmental Affairs
 Federal Financial Management, Government Information, and International Security Subcommittee
 "Cyber Security: Recovery and Reconstitution of Critical Networks"
 July 28, 2006
 Under Secretary George Foresman

Response: The DHS Chief Information Officer (CIO) has agreed to utilize Einstein inside the Department and plans are underway to start the deployment.

The GAO is suggesting that Congress consider clarifying the legal framework guiding Internet recovery. The GAO is also making recommendations to the Secretary of DHS to strengthen the department's ability to serve as a focal point for helping to recover from Internet disruptions by completing key plans and activities and addressing them.

3. Do DHS and the White House concur with these recommendations? If so, how would the authorities given to the President in the Communications Act of 1934 be updated to address the challenges of Internet recovery?

Response: As mentioned, DHS's operating authorities with respect to the cyber security and disaster and emergency assistance missions are grounded in the Homeland Security Act of 2002, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, and executive directives and orders including, but not limited to, Homeland Security Presidential Directives (HSPDs) 5 and 7 and Executive Orders 12472 and 12656, as amended. These authorities are further developed in guidance set forth in policy documents including the National Strategy for Homeland Security, the National Strategy to Secure Cyberspace, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the National Response Plan, and the National Infrastructure Protection Plan (NIPP). While none of these mandates articulates Internet recovery specifically, they provide part of the framework for the efforts that DHS is undertaking with its public, private, and international partners to address risk management and incident response.

Another part of that framework is Section 706 of the Communications Act of 1934, as amended. Our present analysis of the relevant provisions of this section leads us to believe that the President's existing statutory authorities over wireline and wireless communications media would give him significant powers under certain specified circumstances (*i.e.*, wartime or threat of war) to respond to an Internet disruption. Any recommendations for specific changes and/or updates to this provision, or other sections of the Communications Act, will require further legal and policy analysis and discussions among all the relevant stakeholders. We welcome the opportunity to work with Congress and our partners to analyze the legislative environment and determine what, if any, further legislative initiatives may be beneficial for addressing the national cyber and communications risk, response, and recovery efforts.

Cyber Security: Recovery and Reconstitution of Critical Networks**July 28, 2006**

Richard C. Schaeffer, Director of Information Assurance, NSA

Answers to Questions for Response

1. Please identify for the Committee the greatest threats to the Internet in terms of foreign intelligence services, terrorist organizations and organized crime and their capabilities to disrupt, attack, or misuse the network in ways which would be detrimental to the nation.

In a networked world, the barriers for entry into the technical exploitation and attack business are negligible compared to what they were when dedicated systems and point-to-point communications were the rule. Today, any nation state, terrorist organization, criminal enterprise, or disaffected individual needs only Internet access and modest computer science talent to remotely reconnoiter and attempt to manipulate computers and computer-controlled systems with ties to American economic and security interests. As the daily headlines attest, vulnerabilities in commodity information technology (IT) and unfortunate choices on the part of network operators and users routinely invite and enable such mischief. We will always have to guard against the high-end threats posed by the few unusually able and determined adversaries who are willing to mount complex, long-term operations to infiltrate critical networks. However, the greatest threat today though arises from the many low cost, low risk opportunities for adversaries to remotely search for network weaknesses and, sooner or later, parlay a meager investment into disproportionately potent political, financial, or military effects.

Foreign intelligence services are judged to pose the serious threat to the U.S. networks connected to the Internet. Also, sophisticated foreign intelligence services can leverage their traditional intelligence tradecraft, bringing multifaceted capabilities to support their Computer Network Operations.

Terrorist organizations have come to appreciate the value of the Internet and make great use of it for their own communications, research and propaganda purposes. Islamic extremists have been involved in Web page defacement/denial of service attacks, as in their response to the controversial cartoons published in Danish newspapers in early 2006. Some groups do have computer-literate personnel who could be used to conduct such operations.

2. Hypothetically speaking and given NSA's limited authority, what role can/should or does NSA play or wish to play in bringing to bear the significant capabilities it has on improving the security of the network? In other words, what therefore can NSA do to provide enhanced security to all users of the network throughout the nation?

The NSA has unique insight into the vulnerabilities of information systems and the components that comprise those systems, how adversaries can and do operate against them, and how various adversaries and attacks might be best countered. In the days when the national security systems that NSA is explicitly charged to help protect consisted mostly of government-specific components, the NSA had little reason or ability to contribute to the security of unclassified systems or commercial technology. Today, national security systems often rely on commercial products or infrastructure, or interact with systems that do. This has created important common ground between defense and broader homeland security needs and drives the NSA to work with others to raise the information assurance level of IT products and services generally. Accordingly, we've built, and continue to expand, partnerships with other U.S. government entities, private industry and academia. (Our Statement for the Record gives a few examples). In addition to continuing to produce security solutions for the U.S. national security community as we have in the past for many years, we also aim to translate our unique insight (including knowledge derived from classified activities and other sensitive sources) into design guidance for IT suppliers; acquisition and architectural guidance for IT buyers; best practices and situational awareness for system users and operators; recommended doctrine for security authorities; and tools, techniques, and training for fellow (or, in the case of our academic excellence program, future) security practitioners. Such efforts will continue to grow.

3. Does NSA believe it is possible to provide requisite protection for users (defined as all users: personal, business and government) of the network to assure that they can maintain the confidentiality, integrity, and availability of their communications and data and business transactions? If not, what are the most significant things users can do to resist most of the attacks and reduce the vulnerabilities inherent in the system?

"Perfect security" wasn't attainable even within the narrow and relatively easily protected confines of the national security community in the days before the network revolution. It surely isn't within the reach of all network users today, and won't be tomorrow either. With that said, the situation needn't be as bleak as it often is. Frustratingly, the same networks are often found vulnerable to, or even, actually victimized by, the same attack over and over again, and more frustratingly, even when the attack is well known and adequate protective measures are readily available. This is one area where the NSA's insight is not unique. Any number of public and private entities publish lists of powerful computer security basics – things like using strong passwords, promptly installing all software patches, encrypting data at rest, disabling unused computer processes, and allowing users only those privileges which are essential for the work they need to do. It's analogous to the simple precautions we take to protect our homes, like locking doors and windows and installing deadbolts. For most users and system administrators, disciplined attention to just a few basics can be the difference between inviting trouble and actively discouraging it. Users need to understand the added security risk of self-published information in aggregation on the Internet. They must resist unknown eye-catching applications claiming to bring a diversion to its readers.

4. GAO has reported that critical infrastructures extensively rely on information systems and electronic data to carry out their missions. Could a significant Internet disruption pose a threat to national security by interfering with these critical infrastructures?

Many systems that are critical to the nation's security have some connectivity to the Internet or to utilities, communications services, or other infrastructure that make some use of the Internet. In theory, essential national security operations are designed to not wholly depend on the Internet or any uncontrolled external infrastructure, and to be able to function adequately, although perhaps with some degradation, despite modest outages. The complexity of modern operations and networks, however, probably precludes saying that this is always true in practice. It's not unreasonable to think that a significant and sustained Internet disruption might affect at least a few critical functions immediately, and perhaps impact some more over time as unanticipated "ripple" effects emerged.

5. It seems that nation states and disciplined transnational organizations can employ a high level of tradecraft to hide attacks or create successful attacks that do not cause an operational impact on a government agency or commercial enterprise. How concerned are you that the U/S. is being victimized by such attacks and what if anything can be done to develop tools for detecting, analyzing, and stopping these covert attacks?

It is indeed possible for certain types of network intrusions to go undetected for quite some time, and such attacks are of great concern across and beyond the national security community. The threat is being addressed on three fronts. First, both the public and private sectors continue to invest in improving intrusion detection technology. No one pretends that this alone will solve the problem, but progress is being made and every step forward raises our adversaries' operational costs and risks. Second, the public and private sectors also continue to invest in making information technology less vulnerable to unauthorized remote access. Again, we're not going to make attacks impossible, but we can push potential adversaries towards fewer and more demanding attack vectors, and this makes the detection problem more tractable. Finally, it's important to remember that although the problem is tied to technology, the solution need not be. Our efforts to spot and stop attackers at our cyber perimeters must be augmented with aggressive intelligence collection and all source analysis aimed at uncovering our adversaries' plans and capabilities and compromising their operations. Intelligence has long been used in this way to bolster the nation's counterespionage capabilities and to help warn of conventional military attack. It must similarly be a component of our cyber defense.

QUESTIONS AND RESPONSES FROM KAREN EVANS, ADMINISTRATOR FOR
ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY,
OFFICE OF MANAGEMENT AND BUDGET

1. Not that long ago, the federal government's critical infrastructure protection (CIP) coordination efforts were run out of the White House and some in the private sector viewed this as a higher administration priority then as it is now. Should CIP initiatives remain with DHS? Should we consider this prior model?

A: Although there was previously the President's Critical Infrastructure Protection Board, the Homeland Security Act of 2002 assigned DHS the responsibility to develop a comprehensive national plan for securing critical infrastructure and key resources.

In Homeland Security Presidential Directive (HSPD-7) the President designated the Secretary of Homeland Security as the "principal Federal officer to lead critical infrastructure/key resource protection efforts among Federal departments and agencies, State and local governments, and the private sector" and assigned responsibility for critical infrastructure/key resource sectors to specific sector specific agencies. In addition, HSPD-7 assigns the Secretary the role of maintaining an organization to serve as the focal point for securing cyber space and supported by Federal agencies with cyber expertise.

DHS has made critical infrastructure protection a high priority and the release of the National Infrastructure Protection Plan is a significant step in advancing critical infrastructure protection.

The Executive Office of the President, which includes OMB as well as the Homeland Security Council, exercises oversight over DHS programs and we believe the placement of the Assistant Secretary for Infrastructure Protection and the Assistant Secretary for Cyber and Telecommunications in the same directorate within DHS allows for closer integration of cyber and physical security.

2. In your opinion, how important is it for DHS to fill the position of Assistant Secretary for Cyber Security in order to provide the necessary leadership for establishing the plan to recover from Internet disruptions?

A: DHS is currently working with the White House to actively pursue qualified candidates for the post of Assistant Secretary for Cyber Security and Telecommunications. The DHS Under Secretary for Preparedness, George W. Foresman, is personally engaged in the process of selecting the new Assistant Secretary. In the interim, he is providing program direction pending the post being filled permanently. Because of the importance of this mission, all parties want to ensure that the individual appointed to this position possesses the right combination of skills, experience, and leadership necessary to succeed.

To supplement Under Secretary Foresman's involvement, the Assistant Secretary for Infrastructure Protection has been serving as the Acting Assistant Secretary for Cyber Security and Telecommunications. As such, he has been actively engaged in overseeing operational programs, program reviews, governance structure, and has participated in government/industry forums to further the advancement of this important new office.

Regardless of when this position is filled, the mission of DHS, the National Cyber Security Division (NCSD), and the National Communications System (NCS) remain clear. The absence of a permanent Assistant Secretary for Cyber Security and Telecommunication has not had an impact on NCSD's or NCS's critically important work.

3. If Congress were to clarify the legal framework guiding Internet recovery, do you foresee any constructive changes to the Federal Information Security Management Act (FISMA)? Since no private sector firms have embraced FISMA as a "best practice" approach to information security, do you think it's time to craft legislation that actually promotes and measures improvements to security and mandate it for the private sector?

A: We believe existing laws, policy and guidance for securing Federal information systems are generally adequate although the President's Identity Theft Task Force is now looking at possible policy clarifications concerning data breach notification.

FISMA is a valuable tool in improving the state of Federal IT security – both the security of systems and promoting the protection of information.

Our annual FISMA report to Congress highlights key areas of government-wide progress, outlines mechanisms to improve government-wide IT security programs, and provides an update of individual agency implementation status.

The specific security controls used by the Federal government (as set forth by NIST standards and guidelines -- a key feature of FISMA) are derived from and often used by the private sector. The remaining provisions of FISMA, e.g., those regarding oversight, program management, budgeting, reporting, and independent Inspector General evaluations, are specifically tailored for use within the Executive branch agencies. Overall, we favor industry's voluntary adoption of best practices consistent with their unique needs.

[Additional information on FISMA](#)

FISMA assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security.

FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. As such, agencies have the responsibility of managing the security of their systems and Internet gateways in accordance with national security policy and NIST standards and guidance to ensure systems are operating efficiently and have been appropriately secured based on the level of risk assigned. The process for certifying and accrediting information systems is important because it encapsulates the security process. It includes assessing risk, developing plans to manage the risk, implementing and testing security controls to ensure they work as intended, and requires an agency manager to verify they understand any residual risk prior to authorizing system operations. In the process of certifying and accrediting systems, agencies are required to identify system boundaries and interconnections (this includes identifying and securing Internet gateways), implement policies and procedures for system authentication and access control (e.g. password management), and provide for the continuous monitoring of systems.

Additionally, input from the agency IGs is a crucial piece of the annual FISMA evaluation. In addition to assessment and comments in key performance metric areas, OMB annual FISMA reporting guidance asks IGs to assess the quality of the agency Certification and Accreditation process.

4. Why is there such an apparent disconnect between the scores OMB gives to agencies for their compliance with the cyber security goals of the President's Management Agenda (PMA) and the scores agencies receive for FISMA? Since PMA scoring is based on self-reporting and FISMA employs the independent judgment of the IG community, is there a lack of accuracy in PMA reporting?

A: There is a key distinction between these two processes. Congress focuses solely on security performance while the PMA scorecard measures five areas of agencies' performance in electronic government, only one of which is security. Further, the PMA scorecard measures a subset of FISMA's requirements. Specifically they are:

- The percent of agency IT systems properly secured (certified and accredited).
- The quality of the certification and accreditation process as determined by the agency Inspector General;
- Whether the agency Inspector General or Agency Head verifies the effectiveness of the Department-wide IT security remediation process; and
- Has IT systems installed and maintained in accordance with security configurations.

Additional background information on the scorecard

OMB has increased executive level accountability for security by including it in the President's Management Agenda scorecard.

The PMA was launched in August 2001 as a strategy for improving the performance of the Federal government. The PMA includes five government-wide initiatives, including Expanded Electronic Government (E-Government).

Each quarter, agencies provide updates to OMB on their efforts to meet government-wide goals. The updates are used to rate agency progress and status as either green (agency meets all the standards for success), yellow (agency has achieved intermediate levels of performance in all the criteria), or red (agencies have any one of a number of serious flaws).

Information technology security is one of a number of critical components agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot improve their status on the scorecard, regardless of their performance against other E-Government criteria. Agencies are publicly accountable for meeting the government-wide goals, and scores are posted quarterly at <http://results.gov/agenda/scorecard.html>

5. Since 2003, GAO has designated cyber critical infrastructure protection as high-risk area. What is OMB's corrective action plan for addressing this issue? What are you going to do to address the challenges identified by GAO in developing a joint private/public Internet recovery plan?

A: OMB, in coordination with DHS, has prepared an action plan to address Federal information security and the Nation's Critical Infrastructures. This action plan has been shared with GAO. I would be pleased to send the committee a copy of this plan.

DHS can speak to the challenges associated with developing a joint private/public Internet recovery plan.

Additional information on the High Risk Plan

OMB is on track with its improvement plan.

Identified goals have been reached for two out of eleven performance measures:

- The percentage of systems assigned a risk impact level is 92%. The FY06 goal was 80%.
- IGs at 18 out of 25 agencies have verified agency oversight of contractor systems. The FY06 goal was 18 agencies.

Improvements in performance have been achieved for two out of the nine remaining performance measures:

- Implementation of the Einstein tool
- Planning for the Information Systems Security Line of Business

Decreases in performance have been seen in the following two metrics:

- Testing of security controls
- Testing of contingency plans

Agencies have demonstrated mixed performance on the following metric:

- System certification and accreditation (the overall rate dropped slightly but the rate for high impact systems increased)

There has been no change in the following four metrics:

- IG verification of the plan of action and milestone process
- IG assessment of the certification and accreditation process
- Implementation of security configurations
- Government wide contracts for contractor security hardware, software and services

6. The guidance contained in FISMA seems to suggest that the Federal Government cannot relegate information security to the private sector? What is meant by to “provide information security that support the operations and assets of the agency?” Can the government out-source the responsibility of providing information security for systems supporting its missions and those contractor systems providing similar support functions in light of FISMA?

A: FISMA and OMB’s implementing policies ensure agencies remain responsible and accountable for securing their operations and assets regardless of who performs the operations or physically possesses the assets.

While departments and agencies routinely outsource business operations as well as elements of their IT security activities, agency contracts must reflect FISMA’s requirements and the agency continues to be responsible and accountable. Additionally, outsourced operations including security activities are subject to annual reviews by the agency Inspector General.

7. Under FISMA, the Director of OMB is required to maintain an incident response capability. It is our committee understands that this function is currently performed by the US CERT at DHS. Have you issued a formal memo delegating these authorities to DHS and setting clear expectations for the performance of the US CERT? If so, how would you rate its performance?

A: The designation of US-CERT at DHS is clear and no specific delegation memorandum was necessary. FISMA does not require OMB to maintain an operations center, but assigns the Director responsibility for “overseeing the operation of the Federal information security incident center”. In accordance with Section 202 of the Homeland Security Act of 2002, GSA transferred operation of the Federal Computer Incident Response Center to DHS. Additionally, OMB’s security policies make clear to whom agencies must report incidents.

We have made this clear in a number of ways. For example, in April 2005, OMB distributed to departments and agencies the US-CERT Concept of Operations for Federal Cyber Security Incident Handling advising agencies of their responsibilities to follow the procedures. Each year in OMB’s FISMA reporting guidance, agencies and IGs must provide data on their reporting to US-CERT. Most recently on July 12, 2006, OMB directed agencies to report all incidents to US-CERT [see <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf>].

With respect to expectations, the concept of operations was jointly developed by DHS and representatives of the departments and agencies. It defines the US-CERT products and services available to federal customers tasked with preventing, detecting and responding to cyber incidents, and, it establishes roles, responsibilities, and success factors for US-CERT. I would be happy to provide the Committee with a copy of the US-CERT CONOPS.

US-CERT technical staff is available 24 hours a day 7 days a week to answer questions, provide technical assistance and receive reports of anomalous activity, virus infections or other forms of cyber attack. OMB believes US-CERT processes are mature. OMB is working with those departments and agencies whose reporting is sporadic or at an unusually low level to improve their reporting processes.

Questions for the Record, Senator Tom Carper

1. For the past several years, the GAO has consistently rated that access controls are a significant weakness in federal agency information security. As your office reviews agency security plans and determine whether or not to approve them, how will you determine if the agency has taken the appropriate steps to ensure that there are proper access controls in place?

A: FISMA and OMB policy requires agencies to test system security controls annually. In FY 2005, agencies tested these controls on 72% of all systems. However, it is apparent from the data that agencies are properly prioritizing security control testing, since the percentage of high impact systems tested was appreciably higher, at 83%. OMB continues to track this metric quarterly, by risk impact level, and uses this metric as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

2. What criteria does OMB use in determining the sufficiency of an agency's information security program, and how many full-time employees do you have to conduct these reviews? If an agency has an insufficient program, what are the remediation steps necessary to conform with FISMA and OMB policy?

A: OMB uses the President's Management Agenda scorecard as one of several methods to determine the sufficiency of an agency's information security program.

The PMA was launched in August 2001 as a strategy for improving the performance of the Federal government. The PMA includes five government-wide initiatives, including Expanded Electronic Government (E-Government).

Each quarter, agencies provide updates to OMB on their efforts to meet government-wide goals. The updates are used to rate agency progress and status as either green (agency meets all the standards for success), yellow (agency has achieved intermediate levels of performance in all the criteria), or red (agencies have any one of a number of serious flaws).

Information technology security is one of a number of critical components agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot improve their status on the scorecard, regardless of their performance against other E-Government criteria. Agencies are publicly accountable for meeting the government-wide goals, and scores are posted quarterly at <http://results.gov/agenda/scorecard.html>

The PMA scorecard measures a subset of FISMA's requirements. Specifically they are:

- The percent of agency IT systems properly secured (certified and accredited).
- The quality of the certification and accreditation process as determined by the agency Inspector General;

- Whether the agency Inspector General verifies the effectiveness of the Department-wide IT security remediation process; and
- Has IT systems installed and maintained in accordance with security configurations.

In addition, OMB has integrated information technology security into the capital planning and investment control process to promote greater attention to security as a fundamental management priority. To guide agency resource decisions and assist OMB oversight, OMB Circular A-11 "Preparation, Submission and Execution of the Budget" requires agencies to:

- Report security costs for all information technology investments;
- Document that adequate security controls and costs have been incorporated into the life cycle planning of each investment; and
- Tie the POA&Ms for a system directly to the funding request for the system.

Part 7 (Exhibit 300) of OMB Circular A-11 requires agencies to submit a Capital Asset Plan and Business Case justification for major information technology investments. In their justification, agencies must answer a series of security questions and describe how the investment meets the requirements of the FISMA, OMB policy, and NIST guidelines. The justifications are then evaluated on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

Although my office has subject matter experts for information security, we leverage all resources of OMB, including budget examiners in reviewing agency information security programs.

Each year OMB issues reporting guidance to the agencies in order to acquire the information needed to oversee agency security programs and develop the annual FISMA report. (See OMB Memorandum M-06-20 of July 17th, 2006 "FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" at <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-20.pdf>.) As in the past, this year's guidance included quantitative performance measures for the major provisions of FISMA to help identify agency status and progress.

3. The GAO is suggesting that Congress consider clarifying the legal framework guiding Internet recovery. The GAO is also making recommendations to the Secretary of DHS to strengthen the department's ability to serve as a focal point for helping to recover from Internet disruptions by completing key plans and activities and addressing them.

Do DHS and the White House concur with these recommendations? If so, how would the authorities given to the President in the Communications Act of 1934 be updated to address the challenges of Internet recovery?

A: DHS welcomes the opportunity to work with Congress and our partners to analyze the legislative environment and determine, what, if any, further legislative initiatives may be beneficial for addressing the national cyber and communications risk, response, and recovery efforts. In its comments to GAO on the draft report "Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan", DHS agreed to eight of the GAO recommendations and generally agreed with one. OMB concurs with the DHS response.



QUESTIONS AND RESPONSES FROM KEITH RHODES, CHIEF TECHNOLOGIST AND DIRECTOR,
CENTER FOR TECHNOLOGY AND ENGINEERING,
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

G A O

Accountability • Integrity • Reliability

United States Government Accountability Office
Washington, DC 20548

August 17, 2006

The Honorable Tom Coburn, MD
Chairman
The Honorable Tom Carper
Ranking Member
Subcommittee on Federal Financial Management,
Government Information, and International Security
Committee on Homeland Security
And Governmental Affairs
United States Senate

Subject: *Challenges in Developing a Public/Private Recovery Plan*

This letter responds to your request that we answer questions relating to our recently released report and testimony of July 28, 2006.¹ In that hearing, we discussed challenges in developing a public/private Internet recovery plan. Your questions, along with our responses, follow.

1. *Your report outlines challenges DHS faces in planning for Internet reconstitution. Given the many challenges outlined, what practical steps could DHS take now to begin developing recovery plans?*

DHS could take key steps in the near term that could help with recovery planning. Such steps could include completing the Internet components of the National Response Plan and the National Infrastructure Protection Plan. These plans could be used as a basis to develop a public/private Internet recovery plan that includes input from the private sector and addresses activities we identified in our report, such as providing assistance with the provision of fuel and power, providing access to restricted areas, helping with prioritization, and assisting with funds for backup communications systems. In addition, DHS should move to quickly to fill the position of Assistant Secretary of Cyber Security and Telecommunications.

¹GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006) and GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-06-863T (Washington, D.C.: July 28, 2006).

2. *You described several initiatives DHS is taking regarding Internet reconstitution. Why aren't these initiatives sufficient?*

While these activities are promising, some initiatives are not complete, others lack timelines and priorities, and still others lack effective mechanisms for incorporating lessons learned. Specifically, DHS has developed high-level plans for infrastructure protection and national disaster response, but these plans are not complete and lack support from the private sector. DHS officials also have not yet finalized plans, resources, or milestones for future efforts of the Internet Disruption Working Group. Additionally, DHS has not yet identified which group should be responsible for incorporating lessons learned from recent exercises into its plans and initiatives. Other initiatives to improve the nation's ability to recover from Internet disruptions include working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, the relationships among these initiatives are not evident.

3. *The Business Roundtable recently released a report that addressed Internet reconstitution. What are your views on this report?*

Many of the Business Roundtable report's findings are consistent with our report in recognizing that significant gaps exist in government response plans and that the responsibilities of the multiple organizations that would play a role in recovery are unclear. In addition, many of the recommendations from the Roundtable report are also consistent with our report. However, the report's recommendation to create a panel of subject matter experts duplicates already existing groups like the Internet Disruption Working Group and National Cyber Response Coordination Group.

4. *Should NCS and NCSD be combined?*

DHS officials acknowledged that the current organizational structure has overlapping responsibilities in planning for and recovering from a major Internet disruption. NCSD is responsible for planning and response activities governing information technology, while NCS has the lead for telecommunications. As recommended in our report, DHS should either clarify or combine the overlapping roles and responsibilities between NCS and NCSD in light of the convergence of voice and data communications.

5. *How would legislative changes improve the ability of DHS to develop recovery plans?*

Given the importance of the Internet as a critical infrastructure supporting our nation's communications and commerce, Congress should consider clarifying the legal framework that guides roles and responsibilities for Internet recovery in the event of a major disruption. Legislative changes or additions that clarify government authorities with regard to Internet recovery could improve DHS's ability to develop recovery plans. Existing authorities that grant preference or priority to essential communications remain in force, but have seldom been used—and never for Internet recovery. Thus, it is not clear how effective they would be in improving the ability of

DHS in developing recovery plans. In addition, congressional consideration of revisions or additions to the Stafford Act could improve DHS's ability to provide assistance to private-sector Internet infrastructure owners—the current Act does not authorize assistance to for-profit companies.

6. *You identified as one of the challenges for DHS that the private sector was reluctant to share information on Internet disruptions with DHS. Given the diffuse control of the networks, which you recognize, what information could the private sector share that would be helpful to DHS in managing the internet reconstitution? Can Internet reconstitution ever be managed or must it simply be coordinated?*

The private sector could convey specific information on infrastructure vulnerabilities as well as what it needs from the government to facilitate recovery efforts. Internet reconstitution can be more effectively managed by not only sharing information from the private sector to the government, but also from the government to the private sector. Sharing could include threat assessments and detailed information from exercises that are targeted at specific issues such as root server/top-level domain attacks. Providing this information could help with Internet recovery efforts since the private sector is ultimately responsible for recovery activities.

7. *What investments, if any, has DHS made in communications capabilities that enable the nation to coordinate software fixes in the event that key network functions were lost? Is there unused spectrum that could be utilized to allow vendors to push fixes to federal agencies and critical infrastructure facilities in a time of crisis?*

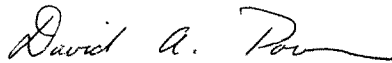
We have not reviewed specific investments DHS has made for these purposes. In addition, we have not reviewed how unused spectrum could be utilized for critical infrastructure protection since these issues were not included in the scope of our work.

8. *The GAO is suggesting that Congress consider clarifying the legal framework guiding Internet recovery. The GAO is also making recommendations to the Secretary of DHS to strengthen the department's ability to serve as a focal point for helping to recover from Internet disruptions by completing key plans and activities and addressing them. Do DHS and the White House concur with these recommendations? If so, how would the authorities given to the President in the Communications Act of 1934 be updated to address the challenges of Internet recovery?*

DHS concurred with our recommendations to the department, and in its written comments, stated that strengthening collaboration is critical to protecting the Internet. Updating key authorities to allow assistance to the private sector during recovery efforts and to clarify roles and responsibilities given the convergence between voice and data communications would help address challenges of Internet recovery.

In responding to these questions, we relied on previous audit work we preformed in developing our report on Internet recovery. Should you or your office have any questions on matters discussed in this letter, please contact us at (202) 512-9286 or (202) 512-6412, or by email at pownerd@gao.gov and rhodesk@gao.gov.

Sincerely yours,



David A. Powner
Director, Information Technology
Management Issues



Keith A. Rhodes
Chief Technologist and Director,
Center for Technology and Engineering

QUESTIONS AND RESPONSES FROM ROBERTA A. BIENFAIT,
SENIOR VICE PRESIDENT, GLOBAL NETWORK OPERATIONS, AT&T

U.S. Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on Federal Financial Management,
Governmental Information, and International Security

1. Do you agree with the GAO assertion that private industry has developed a reasonable level of competency in restoring their portion of the Internet? A recent report by the Business Roundtable identified gaps in the abilities of both the government and private sector in responding to Internet disruptions. Are private sector efforts in Internet recovery planning sufficient? Are there cases where private industry needs DHS' help in restoring their portions of the Internet Infrastructure? What is the appropriate role of government in Internet recovery planning?

Answer: First and foremost, we do not believe that the Internet should be treated separately from the overall communications and IT infrastructure. The Internet and communications based on Internet Protocol (IP) are in actuality an integral part of that infrastructure, and all Internet Service Providers - including AT&T - rely on the functioning of the overall infrastructure to deliver service.

Private Sector efforts have been adequate in addressing the events we have experienced to date. However, we have been fortunate that there has been no event with sufficient impact to cripple the entire communications/IT infrastructure. Thus far, the events we have encountered had impacts of varying significance to the providers and users of the infrastructure, in large part due to the nature of the event, the various protective measures employed by service providers and users, and the products and IT services that the event targeted. While some individual websites, databases and enterprise LANs have been severely impacted by a single event, other service users and providers were mostly or entirely unaffected. We have yet to have an event of such universal impact and impairment of other critical infrastructures to rise to the level of an event of national significance. Even 9-11 and Hurricane Katrina were local events that impaired cyber functionality in a confined area with no impact at the national level.

Also, we do not believe that all segments of the private sector that rely on the communications and IT infrastructure are prepared for a major cyber or physical hit to that infrastructure. Despite the devastating effects of Hurricanes Katrina and Rita last year, nearly half of the 1,000 companies recently polled by AT&T also said that they do not take specific protective actions even when state or federal governments issue warnings for an impending disaster, such as severe weather.

Specific to recovery from a disaster of cyber incident, different sectors of the private sector have varying levels of assistance they might require from DHS. In our policy recommendation we included several areas where AT&T needs DHS support including:

- Furnish standardized and approved emergency credentials to vital communications and other infrastructure providers in advance, so that AT&T and other specialized disaster staff can get into affected areas to restore vital capabilities without delay or interference.
- Predetermine security needs and formalize request process from telecommunications carriers for law enforcement deployment to protect critical infrastructure facilities immediately following a disaster.

In the larger sense, DHS and the Federal Government can play a key role in stimulating research and development of more-secure products and services, including the ability to detect and respond to cyber attacks. The Federal Government can also stimulate the deployment of more-secure products and services through its purchasing power as a user of more secure and robust cyber capabilities.

2. In your opinion are the communications infrastructures destroyed by Hurricane Katrina critical infrastructures as the DPA defines them, and if so, which if any part of these infrastructures could be a part of the Internet Infrastructure?

Answer: Critical infrastructure is defined by the DPA at 50 US App. § 2152 as “any systems and assets, whether physical or cyber-based, so vital to the United States that the degradation or destruction of such systems and assets would have a debilitating impact on national security, including, but not limited to, national economic security and national public health or safety.” The DHS, DoD, or the carriers that suffered major damage from Katrina would have a better picture of the specific impact from Hurricane Katrina as it relates to the DPA criteria. We believe that components of the communications infrastructure clearly would meet the definition of critical infrastructure as defined under DPA, and are in fact essential to the function of other critical infrastructures. The agencies or private sector companies that have the responsibility for providing the services that utilize this critical infrastructure have the responsibility to identify them and to protect them using continuity principles and practices including restoration priority identification under TSP. Also, as we discussed in our answer to Question 1, we do not believe it makes sense to differentiate communications infrastructure from Internet Infrastructure – IP convergence has made them one and the same.

3. The GAO found that private industry indicated it had a handle on Internet Recovery of its portion of the Internet. The report goes on to suggest that private industry sees a more limited role of DHS in Internet recovery at the present time. One suggestion is that DHS narrow its focus to government owned or controlled critical infrastructures. How do you see the law addressing situations where the communications system or assets are deemed critical but are not government owned, such as when they are purchased or leased from a private vendor?

Answer: As the customer, they have the ability to assess and verify that their suppliers are capable of meeting their requirements, including recovery of their infrastructure. They have the ability to purchase their services and infrastructure only from the vendors that are able to clearly demonstrate they can provide the reliable and robust services required by the government.

4. What are the risks and benefits to your firm of sharing information with DHS? What improvements could DHS make in building an information-sharing relationship with your company?

Answer: Since we operate in a highly competitive marketplace, communications carriers must have a compelling business case to support information sharing with DHS or any other entity. There must be a concise definition of the type of information to be shared, the purposes for which the information will be used, how that information will be handled and protected from disclosure, and what will be provided back to the carrier as a result. In other words, the sharing must result in a trusted relationship which reassures industry of minimal risk to our proprietary information and our competitive position in the marketplace. All of these are essential to any discussion of information sharing.

Following our answers, we have attached a listing of some of the categories of information that have come up in information sharing discussions. To accurately address the issues surrounding information sharing, one must confine the discussion to each of these categories separately. The desires, concerns and issues of both government and the private sector may be unique to each of these categories.

5. How have DHS's leadership and organization issues impacted its effectiveness in working with private-sector firms?

Answer: We believe we work effectively with DHS at all levels and throughout all of the DHS agencies. However, rapid turnover of leadership in the past, along with resultant changes in priorities, have impacted follow-through on some new initiatives, or disrupted ongoing successful programs. We believe that stabilization of leadership at

DHS, with consistently applied priorities and funding for programs, will enhance our ability to work on strategic initiatives as well as individual programs.

6. What are some legislative barriers to the government assisting private-sector firms in recovering from major disruptions to the Internet?

Answer: There are different interpretations of the Robert T. Stafford Disaster Relief and Emergency Assistance Act as industry learned during the Hurricane Katrina response and for infrastructure. Some believe that it is fine for disaster recovery in the context of natural disasters, but not for critical infrastructure protection or recovery outside of natural disasters. In reading the Stafford Act, there may be some confusion regarding the focus around the definition of "Major Disaster." For the Stafford Act, "Major Disaster" means any natural catastrophe (including any hurricane, tornado, storm, high water, wind driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby." It might be easy to argue that while the major disaster was reasonably specific to natural disasters *"regardless of cause, any fire, flood, or explosion"* would clearly cover any physical terrorist act since most would involve a fire or explosion like the attacks on the WTC. This definition of "Major Disaster" does not seem to cover cyber events like denial of service attacks. The definition for "Major Disaster" should be updated to include some of the cyber events that are likely to disrupt the cyber infrastructure.

We also support the recommendation by the National Security Telecommunications Advisory Committee to the President, that communications sector workers be formally designated as Emergency Responders.

7. Please describe the involvement of private-sector firms in development of the recently released National Infrastructure Protection Plan and your views of the efforts to develop this plan. Does the current proposed version of the National Infrastructure Protection Plan present a clear, actionable and deployable solution for the private sector to follow to secure critical infrastructures? Is DHS taking the right approach (e.g., all hazards)?

Answer: The combination of the NIPP plus other resources available from Government Agencies (e.g. FEMA 427 Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, FEMA 452 Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, www.ready.gov, FEMA FPC 65 Continuity of

Operations, National Institute of Standards and Technology Contingency Planning Guide for Information Technology Systems, etc.) provide a very useful framework for both public and private sector continuity and contingency planning. Appendix 5B (Recommended Homeland Security Practices for Use by the Private Sector) of the NIPP includes an excellent summary of practices that should be adopted by private sector entities.

The “all hazards” approach is a very prudent approach to continuity and disaster planning. In most cases it might not matter why your place of business was destroyed. The fact that it was destroyed and you need to have an alternate means to support your business is the key. Each emergency situation presents its own unique set of challenges, and even the most thorough planning cannot take the place of ingenuity and resourcefulness when the unforeseen happens. That said, much can be anticipated and we must plan and drill to address a variety of events on any scale. Planning, exercising, and drilling for an “all hazards” event presents the best opportunity for recoverability.

As a high-level plan that must address all infrastructures, the NIPP is a good baseline for the Critical Infrastructure Protection (CIP) mission. We are currently supporting our Sector Specific Agency (SSA), through our Communications Sector Coordinating Council, in creating the second draft of the Sector Specific Plan (SSP). This document will deal with individual sectors at a level of detail to address the unique characteristics and requirements of each sector. For this reason, the development of an accurate and useful SSP is significantly more important to industry than the NIPP.

8. What effect will the naming of an Assistant Secretary for Cyber Security and Telecommunications have on your industry? What authorities will best enable the new Assistant Secretary to successfully perform his job? Are they currently in place?

Answer: The key to this leadership role is the potential to coalesce the various aspects of communications and information technology into a single focus area - convergence has made the traditional distinctions between the Public Switched Network and the Internet obsolete. Another area that must be addressed is the traditional separation of response and incident management mechanisms for physical and cyber threats as pertains to the Communications/IT infrastructure. We are hopeful that the new Assistant Secretary will bring the vision and foresight to get a clear grasp of these issues and then articulate the appropriate means for addressing them. The DHS organizational structure and authorities can then be defined and aligned in a way that makes sense.

9. The Business Round Table report refers to Tripwires. Is advanced or early warning really possible given the speed of cyber attacks, or do you simply mean that we need thresholds for when significant government involvement may be necessary?

Answer: We believe the “Tripwires” referred to in the Business Round Table report primarily deal with the ability to detect the early stages of a cyber-attack – a cyber early warning system. A large part of this challenge is to differentiate “normal” cyber activity, such a spam, pfishing, worms, and localized denial of service attacks, from a large-scale, concerted cyber attack aimed at a significant disruption of our communications and information technology infrastructure. Achieving this requires that appropriate alerting information is shared in real-time between the various communications service providers, and that response coordination mechanisms be created, including Government Authorities, such as DHS. Our answer to Question 4 above also applies here.

10. During a large scale disruption of the internet would your vendors have sufficient resources to assist you in recovery? If multiple members of the infrastructure also required their assistance at the same time?

Answer: This question is difficult to answer without identifying what is meant by a large scale disruption, and the type of disruption experienced. As described in our testimony to the Subcommittee, AT&T has extensive plans and capabilities for Network Disaster Recovery, primarily aimed at physical events. We also have an extensive capability to detect cyber attacks against our core network and our customers, and to deal with these events on the scale of what constitutes “normal” in today’s world. Events that transcend the entire infrastructure, and/or overwhelmed our corporate capabilities, would be another matter.

Government truly has a role when there is a contention for resources to respond to a nationally significant event. Arguably, the required authorities currently exist through various Executive Orders and the Communications Act of 1996 that provide for the Joint Telecommunications Resources Board (JTRB) and the President to exercise the authority to allocate those resources. AT&T participates in this process with DHS and the White House through the National Coordinating Center (NCC).

11. Has your infrastructure discussed restoration priorities with your service providers? With the responsible government agencies (FEMA, NCS, SEC, etc.)?

Answer: AT&T follows the Telecommunications Service Priorities (TSP) program as mandated by the FCC through its Report and Order in the matter of TSP in Docket 88-341.

12. Have you participated in detailed table top exercises that incorporate multidiscipline and multi-infrastructure participation to walk through potential large scale internet disruptions and the resultant recovery efforts and impacts on civilians?

Answer: We participated in the U.S. Department of Homeland Security's Top Officials Three Exercise (TOPOFF 3). The TOPOFF 3 Exercise Program, the most comprehensive terrorism response exercise ever conducted in the United States, is made up of a two-year cycle of seminars, planning events and exercises culminating in a Full-Scale Exercise that simulates a coordinated terrorist attack involving biological and chemical weapons. The Full-Scale Exercise took place April 4–8, 2005. TOPOFF 3 is managed by the U.S. Department of Homeland Security's Office of State and Local Government Coordination and Preparedness, and involved numerous Federal departments and agencies, the states of Connecticut and New Jersey, the United Kingdom, Canada, and representatives from the private sector.

AT&T also participated in the DHS NCS-D Internet Disruption Working Group tabletop exercise on June 15, 2006.

13. During a large scale disruption of the internet how would your infrastructure communicate with its members? With other infrastructures? With the local government? With the federal government?

Answer: AT&T has implemented multiple layers of emergency communications including the use of HF repeaters and radios to communicate internally and externally. Our testimony included in our policy recommendations a suggestion to designate a lead agency in the Federal Government that would coordinate planning including the emergency communications protocol for any disruption. The agency that is designated as the National Cyber Incident Commander must also be the lead for the planning and exercising of coordinated response plans with all parties in the cyber infrastructure. The first items that must be addressed immediately by this agency are a coordinated advanced warning mechanism including an emergency communications plan. This coordinated advanced warning mechanism should be a way of identifying potential emergencies and agreed-upon protocols and thresholds that indicate an attack is under way or a disruption is imminent. An emergency communications plan must address the protocols and processes for responding to severe failures as well as the infrastructure used to communicate.

Our current view is that the NCC is the vehicle for interfacing with the members of our infrastructure and with the government for disaster recovery. The NCC administers the SHARED RESOURCES (SHARES) High Frequency (HF) Radio Program, and until recently, the Alerting and Coordination Network (ACN), which could be vital elements of a

survivable sub-infrastructure to support emergency communications in the face of a large scale disruption of normal communication services.

14. During the recovery from a large scale disruption of the internet how is your infrastructure sure that their recovery plans won't introduce additional vulnerabilities into the infrastructure itself?

Answer: AT&T takes our responsibility for operating secure and reliable networks very seriously. Our network design goal is to have a network where failures are prevented, or predicted and pro-actively corrected, before they impact a customer's service. This goal is the foundation for the preventive, predictive, and proactive efforts that we take to first protect our physical and virtual infrastructure and second to be able to restore this infrastructure under any circumstances. We have undertaken a program that includes both rigorous exercising and an extensive research component to verify our restoration and recovery plans work.

15. Given the importance of the Internet as a critical infrastructure supporting our nation's communications and commerce, what is deemed a critical network or part of the Internet? Should there be minimum essential criteria to identify, define, and characterize critical infrastructures? Is restoring local communication systems part of critical infrastructures protection or are they government owned systems or assets?

Answer: The Internet is a network of networks, both private and government-owned. Moreover, convergence has made distinctions between the public Internet and other communications services increasingly immaterial. Many large businesses, for example, maintain IP-based enterprise infrastructure based on network services provided by carriers, as do many federal, state and local government agencies. And an increasing amount of voice communications now traverse the Internet in whole or in part. One great benefit of the Internet structure is the ability dynamically to route around problems. Nonetheless, each of the large private Internet backbone owners maintains certain facilities that carry substantial Internet traffic and has established private "peering" points of interconnection to exchange traffic with the other backbone providers. Given the dynamic nature of the Internet, the operators are in the best position to determine which facilities are critical infrastructures at any point in time, and it would likely be difficult to craft definitions or criteria that would keep pace with new developments. But it is clear that the Internet is critical to supporting our nation's communications and commerce and that appropriate disaster prevention and disaster recovery efforts are essential. A major disruption of "Internet" operations would have a dramatic impact on all communications services in the United States, not just those viewed as Internet services.

As was also vividly demonstrated during Hurricanes Katrina and Rita, many local wireless systems, owned by both local governments and private sector providers, are also critical assets, particularly in times of emergency.

Many cyber-attacks today involve multiple home or business computers that have been electronically captured by distant hackers, and used to launch denial of service and other attacks. Cyber security is thus a distributed problem and not restricted to the elements that are a part of the public infrastructure. Computing and communication devices and software are now present in the commercially-provided infrastructure, the enterprise network, and the end user device. Each has the potential to affect the others. This is also true between the interconnected providers of the infrastructure. While we understand the desire to come up with a simple method of identifying and prioritizing critical infrastructure, this is an extremely complex task.

16. How do these restoration priorities correspond with the infrastructures determination of "critical assets"? For instance, during Katrina several substations' priority levels were raised because it turned out they supplied power to critical pipelines. Yet the electric sector did not have these small remote substations as "critical". How can we be sure that other such items don't fall through the cracks?

Answer: We recommend that DHS investigate expanding the role of the ISACs to provide greater exchange between the Communications ISAC, the Electric Service ISAC, and the State and Local Governments to ensure the TESP provides comprehensive coverage of electrical restoration priorities in support of communications infrastructure needs.

Some Information Sharing Categories

Incident Report: An incident report is a report that an “all hazards” incident has occurred and should include such details as what occurred, where it occurred, and when it occurred. The impact or consequences of the event will be reported as “situational awareness”

Threat Warning: A threat warning is information pertaining to an existing or developing threat posing the potential for an incident to occur. A warning should be specific and actionable rather merely stating a general concern of a potential event. Warning should pertain to events which are imminent.

Risk Data: Risk data pertains to the information regarding the potential consequences to assets, functions or services at risk should the incident under study actually occur.

Vulnerability Data: Vulnerability data is information pertaining to the assessment of the degree to which given assets, functions or services are vulnerable to the threat posed by the potential incident being studied.

Advisories: Advisories are formal, narrative information bulletins intended to advise the recipient of certain facts, such as new threat information, the occurrence of an incident, etc.

Alerts: An alert is an advisory of an urgent nature. While an advisory notifies and informs, the alert is a call to action.

Analytical Products: Analytical products are the documented conclusions of the government intelligence community and other subject matter experts (SMEs) derived from the application of threat information against known or perceived vulnerabilities to determine the potential of occurrence and the consequences from such an occurrence.

Raw Asset Data: Raw asset data is a list of assets and the locations of those assets which, in the context of CIP, are the building blocks of a critical infrastructure.

Situational Awareness: Situational awareness refers to the impact analysis and assessment of the effects of an event on the impacted assets and infrastructure, including the consequential impacts on other infrastructures, functions and missions.

Responses of Michael A. Aisenberg to Questions posed by the Committee

1. Do you agree with the GAO assertion that private industry has developed a reasonable level of competency in restoring their portion of the Internet? A recent report by the Business Roundtable identified gaps in the abilities of both the government and private sector in responding to Internet disruptions. Are private sector efforts in Internet recovery planning sufficient? Are there cases where private industry needs DHS' help in restoring their portions of the Internet Infrastructure? What is the appropriate role of government in Internet recovery planning?

From VeriSign's perspective as an infrastructure steward and service provider, we have significant confidence in our competency to maintain and restore our service levels in the face of exploits. These capabilities have, however, largely been developed with limited or no involvement from government, including DHS/NCSD/NCS and its predecessor agencies (e.g., NIPC, DISA). As a result, we observe two facts: (1) there is at present little opportunity for government operators of parallel network infrastructures to learn the techniques we rely on to maintain and restore our CI services; and, (2) no pre-ordained path for information sharing regarding sensitive exploits/attacks. (see questions 4 and 9 below).

2. In your opinion are the communications infrastructures destroyed by Hurricane Katrina critical infrastructures as the DPA defines them, and if so, which if any part of these infrastructures could be a part of the Internet Infrastructure?

Using a broad understanding of "infrastructure" in a converged/NGN sense, many of the at-risk infrastructures (e.g., BellSo switches) are part of the "Internet Infrastructure".

3. The GAO found that private industry indicated it had a handle on Internet Recovery of its portion of the Internet. The report goes on to suggest that private industry sees a more limited role of DHS in Internet recovery at the present time.

One suggestion is that DHS narrow its focus to government owned or controlled critical infrastructures. How do you see the law addressing situations where the communications system or assets are deemed critical but are not government owned, such as when they are purchased or leased from a private vendor?

Most b-to-b service provision in the private sector is a matter of contract and thus not appropriate for further statutory constraint. With respect to public-private collaboration for restoration of truly CRITICAL INFRASTRUCTURES (e.g., service to stock exchanges, banks, first responders, health care, transportation (ATC)) and essential government services, as well as government networks), policy clarification could assist in the areas of:

- defining shared roles and responsibilities
- establishing protocols for information sharing
- establishing processes/procedures for restoration/recovery
- defining incentives to improve lagging private sector practice
- establish fast track process to improve government network management

practices

4. What are the risks and benefits to your firm of sharing information with DHS?

What improvements could DHS make in building an information-sharing relationship with your company?

Direct pathway to NCRCG process for "cyber incident of national significance."

5. How have DHS' leadership and organization issues impacted its effectiveness in working with private-sector firms?

The continuing lack of unified leadership over NCSD-NCS has been a continuing and distracting preoccupation for industry. These adverse impacts have been remedied in part by effective and aggressive effort at cooperation by Asst. Sec. Robert Stephan and his staff, in part by aggressive

work by industry to seek out DHS engagements and overcome these negative impacts, and in part by the diligence of NCSD and NCS leadership.

6. What are some legislative barriers to the government assisting private-sector firms in recovering from major disruptions to the Internet? Congress has yet to address the issue of federal jurisdiction over (previously unregulated) "Internet" service providers in the IP environment. Under the Pulver line of cases at the FCC, there is an assumption that some jurisdiction exists for imposition of certain obligations on ISPs offering "information services" under Title I of the communications Act. This view is not uniformly accepted by the Internet community and has yet to be tested in the courts.

7. Please describe the involvement of private-sector firms in development of the recently released *National Infrastructure Protection Plan* and your views of the efforts to develop this plan. Does the current proposed version of the National Infrastructure Protection Plan present a clear, actionable and deployable solution for the private sector to follow to secure critical infrastructures? Is DHS taking the right approach (e.g., all hazards)?

Since the summer of 2005, new DHS IA/IP leadership has: "rescinded" prior NIPP drafts whose content concerned industry, worked with industry to develop a responsive, inclusive drafting process, has solicited and received editorial input from Internet industry directly and through industry organizations, as well as economy-wide representation (PCIS, e.g.) and existing advisory committees (NSTAC, NIAC) and published a NIPP substantially more reflective of industry concerns. The follow-on Sector Specific Plan process is continuing the open, inclusive and responsive model, collaboratively led by Sector Coordinating Councils and their government peers, and promises to be significantly closer to the concerns of individual sectors. It is defined as "iterative" and a "work in progress" which will be subject to continuous improvement. The "correctness" of DHS' approach, at least regarding the ICT sectors, will be revealed when put to an operational test during an exploit.

8. What effect will the naming of an Assistant Secretary for Cyber Security and Telecommunications have on your industry? What authorities will best enable the new Assistant Secretary to successfully perform his job? Are they currently in place?

The ending of uncertainty and distraction engendered by the continuing vacancy of the Assistant Secretary position will be of substantial benefit to industry and DHS in allowing a clearer path for policy development and public-private collaboration on significant national plans, and cooperation in the event of another significant event of national significance. The IT industry will be able to engage with DHS/NCSD-NCC in a clear and unambiguous manner once the question of "who's in charge" gets a clear answer.

9. The Business Round Table report refers to Tripwires. Is advanced or early warning really possible given the speed of cyber attacks, or do you simply mean that we need thresholds for when significant government involvement may be necessary? In general, No. The "zero-day" phenomenon is essentially on us, and the opportunity for "collaboration prior to response" is increasingly rare. The definitional issue of "when does an exploit/attack warrant disclosure to and deliberation/decision by the NCRCG process" deserves examination, and creation of some practical protocol of disclosure, especially from a core group of truly critical infrastructure providers. (number is probably less than 50 Internet/network critical infrastructure entities).

10. During a large scale disruption of the internet would your vendors have sufficient resources to assist you in recovery? If multiple members of the infrastructure also required their assistance at the same time? For DNS, there are few supportive resources available. Indeed, VeriSign is frequently looked to, to assist other DNS providers (registries for .edu, .mil, .gov, for example).

11. Has your infrastructure discussed restoration priorities with your service providers? With the responsible government agencies (FEMA, NCS, SEC, etc.)?

Yes. We have held discussions generally within IDWG, directly with the FCC, with DHS and with NCRCG.

12. Have you participated in detailed table top exercises that incorporate multidiscipline and multi-infrastructure participation to walk through potential large scale internet disruptions and the resultant recovery efforts and impacts on civilians? Yes. Both directly as VeriSign and via industry bodies (IT- ISAC, we have participated) in a variety of exercises, including Internet Disruption working Group, Cyber Storm, TopOff III and IV. These efforts must become continuing, institutionalized and used as a basis for development of policy and change in practice by both industry and government.

13. During a large scale disruption of the internet how would your infrastructure communicate with its members? With other infrastructures? With the local government? With the federal government? This question begs the issue of resiliency of the Internet itself, and the availability of substitute channels in the event of (wide-scale) disruption/outage of IP services. To date, no exploit has disabled both the transport layer and the address system at the same time in a manner to fundamentally 'take down' the network and disable the capacity to notify peer providers, government and other institutions of the pendency of the attack.

14. During the recovery from a large scale disruption of the internet how is your infrastructure sure that their recovery plans won't introduce additional vulnerabilities into the infrastructure itself? This is largely the product of extensive testing and exercising of our infrastructure.

15. Given the importance of the Internet as a critical infrastructure supporting our nation's communications and commerce, what is deemed a critical network or part of the Internet? Should there be minimum essential criteria to identify, define, and characterize critical infrastructures? Is restoring local communication systems part of critical infrastructures protection or are they government owned systems or assets? While the "definition" of "CI" is largely in the eyes of the beholder, we believe a consensus can be reached on the following institutions:

- infrastructure which supports continuity of operations of the network itself
- infrastructure which is essential to continuity of government operations ("CoG")
- infrastructure essential to national security and emergency preparedness/first response
- infrastructure essential to the operation of other critical infrastructures (water, health care, financial services, electric/nuclear power, etc.)

16. How do these restoration priorities correspond with the infrastructures determination of "critical assets"? For instance, during Katrina several substations priority levels were raised because it turned out they supplied power to critical pipelines. Yet the electric sector did not have these small remote substations as "critical". How can we be sure that other such items don't fall through the cracks? There are no presently NO clearly articulated criteria for "critical CYBER/IP assets".

**Responses of Karl Brondell and Business Roundtable to Questions
From the U.S. Senate Subcommittee on Federal Financial
Management, Government Information and International Security
August 18, 2006**

1. Your report refers to Tripwires. Is advanced or early warning really possible given the speed of cyber attacks, or do you simply mean that we need thresholds for when significant government involvement may be necessary?

While Business Roundtable member companies certainly have their own cyber defenses and recovery systems, we know how critical it is to have timely information about a developing attack or spreading Internet outage. No one expects that the U.S. will have several days to prepare for a cyber attack – as we do for major storms – but Roundtable companies do want to know information about whether an attack is occurring and how it is spreading. The more we know – and the faster we know it – the quicker we can arm our defenses and engage our recovery efforts. We are, therefore, fully supportive of industry-led efforts to share information across the business community and the public sector, such as the Information Sharing and Analysis Centers (ISACs). We believe that the Department of Homeland Security's US Computer Readiness Team (US-CERT) plays a similar role essential to manage catastrophic cyber-based disasters.

2. Your recent report identified gaps in the abilities of both the government and private sector in responding to Internet disruptions. Are private sector efforts in Internet recovery planning sufficient?

Companies are already doing a great deal to plan and prepare, but we all need to do a better job in getting ready. Business Roundtable's report – *Essential Steps to Strengthen America's Cyber Terrorism Preparedness* – offers recommendations for individual businesses, the government and for better collaborative public-private planning. The Roundtable report finds that some of these cyber problems are going to be too big for any one company to address in the event of a massive cyber catastrophe. That's why we need to work together on plans to recover the Internet should such a disaster occur.

The Roundtable's report makes several suggestions for businesses.

- Companies are encouraged to designate a point person or position for cyber recovery.
- Businesses are urged to update their strategic plans to prepare for a widespread Internet outage and the impact on movement of goods and services.
- Companies are recommended to set priorities for restoring Internet service and corporate communications.

The Roundtable's next step in this ongoing effort is to work with member companies on the steps that companies will need to take to keep their businesses operating – and what they will need from public and private institutions.

3. What is the appropriate role of the government in Internet recovery planning? Does your infrastructure know what type of assistance they might want from the government and from whom?

This question goes to the heart of Business Roundtable's follow-up work from our recent report: *Essential Steps to Strengthen America's Cyber Terrorism Preparedness*. The Roundtable's Security Task Force is working with member companies to determine – from a business and economic standpoint – what companies need from government in recovering from an Internet catastrophe. One of the key findings from the Roundtable's report is that if there is a cyber disaster, there is no emergency number to call – and no one in place to respond. Our nation simply doesn't have the kind of coordinated plan in place that we need to restart and restore the Internet. The Roundtable report acknowledges that our nation has not experienced – yet – the kind of massive Internet disruption that shuts down large parts of the Internet and one that is so large that no single company or government can recover it. But that doesn't mean we shouldn't have plans in place to deal with this threat.

4. Please describe the involvement of private-sector firms in development of the recently released *National Infrastructure Protection Plan* and your views of the efforts to develop this plan.

Business Roundtable is happy to see that the Department of Homeland Security (DHS) has developed this plan, and thinks it is a step in the right direction. The Roundtable also is pleased to see that the plan recognizes the important role of the private sector, which owns or operates more than 85 percent of the nation's critical infrastructure. The Roundtable – as an organization – had fairly limited input into details of the plan.

5. From an insurance company standpoint, can cyber insurance be an incentive for corporations to upgrade their network security?

My appearance before the Subcommittee was as a representative from Business Roundtable, which does not have a position on this issue. My employer, State Farm, does not do business in this area of insurance.

6. What are the risks and benefits to your firms of sharing information with DHS? What improvements could DHS make in building a relationship with your companies?

Business Roundtable CEOs understand that when it comes to protecting America, business can't do it alone – and neither can government. The best security solutions require business and government to work together. Sharing timely information is a key part of that partnership, especially in disaster response and recovery. That's one of the main reasons that following the 9/11 attacks, the Roundtable created CEO COM LinkSM, a secure system that allows CEOs and top government leaders to exchange information about a threat or major crisis. CEO COM LinkSM can be used to mobilize a national response to a threat or a catastrophe. CEO COM LinkSM is part of the National Response Plan, and the Roundtable knows that DHS is committed to a strong relationship with the Roundtable and the private sector. DHS has had more than half a dozen conversations with the Roundtable in recent weeks – and the intent is to continue that dialogue in the months ahead as we work together to strengthen our nation's preparedness for a major Internet attack or outage. We are especially pleased with the commitments and support received from the Under Secretary of Preparedness, George Foresman in helping Roundtable CEOs navigate across DHS and within the Preparedness Directorate.

7. What are some legislative barriers to the government assisting private-sector firms in recovering from major disruptions to the Internet?

Legislative changes were not the Roundtable's central focus in conducting the work for the report: *Essential Steps to Strengthen America's Cyber Terrorism Preparedness*. Consequently, the Roundtable does not have any specific legislative recommendations at this point. We did, however, assess many of the strategic challenges and impediments that public and private sectors must contend with in reconstituting critical Internet services after a disruption. For example, we conclude that security must be a greater focus in support of industry repair professionals. For instance, Congressional laws covering the Federal government's support for response operations do not cover security support for the private sector.

With regard to legislative issues involving the Federal government institutions essential for reconstituting the Internet, the Roundtable's report noted that the US-CERT needs greater statutory authority to operate and with appropriate funding. If the US-CERT's role and responsibility is better defined and better funded by Congress, then businesses have an agency – that is accountable – to call during a cyber crisis.

The Roundtable report also called on the federal government to establish clearer roles and responsibilities, fund long-term programs on reconstitution, and ensure that national response plans treat major Internet disruptions as a serious national problem. For example, the Administration says that it has authority to declare a cyber emergency and will consult with business leaders, but it is not clear how this consultation will occur or how they will decide whether to declare an emergency. The Roundtable encourages Congress to support changes to law that address these important issues.

If the Roundtable develops specific legislative recommendations in the next phase of its work, we will be happy to pass them along to you.

8. How have DHS's leadership and organization issues impacted its effectiveness in working with private-sector firms?

There is no question that DHS is committed to strengthening our nation's physical security, cyber security and preparedness, and Business Roundtable has worked closely with DHS leaders at all levels to improve the public-private partnership to protect our country. The Roundtable supported the creation of the position of an assistant secretary for cyber security, and we are hopeful that someone can be nominated and confirmed in the near future. As noted above in response to a previous question, we are especially pleased with the commitment and support from the Under Secretary for Preparedness in bridging public and private issues that are the subject of this Congressional hearing.

9. Have you participated in detailed table top exercises that incorporate multi-discipline and multi-infrastructure participation to walk through potential large scale internet disruptions and the resultant recovery efforts and impacts on civilians?

The Roundtable participated in Cyber Storm as an observer and understands the benefit to conducting exercises. In fact, the Roundtable's report – *Essential Steps to Strengthen America's Cyber Terrorism Preparedness* – suggests that DHS and industry conduct large-scale cyber emergency exercises, with lessons learned integrated into programs and procedures. Looking forward, the Roundtable believes that these exercises should focus more clearly on business continuity and recovery – so that at least part of the exercise examines economic recovery and business confidence. The Roundtable believes that the issue is bigger than technology – it's about our nation's economy.